DRI CANADA
Train. Prepare. Recover.
Former • Préparer • Rétablir

ISSN 2816-900X (print)
ISSN 2816-9018 (online)

TRUE NORTH RESILIENCE
Résilience du vrai nord

DRI Canada's magazine / Magazine de DRI Canada

Vol 05 No 1 Spring/Printemps 2026 (8th Edition)

Feature article:
• CODE SILVER SIMULATION
and much more...

Article vedette :
• SIMULATION D'UN CODE ARGENT
et plus encore...

Canadian Publication Agreement Number 44001035
Numéro d'accord de publication canadien 44001035

www.dri.ca

Upcoming Symposium
Symposium à venir

DRIC symposiums are one-day events specifically designed for senior-level business continuity, disaster recovery, cyber resilience and risk management professionals. They aim to provide a dynamic and interactive platform for leaders to explore innovative strategies, share best practices, and discuss the latest trends in business continuity management.

During these immersive events, participants can engage with like-minded professionals and thought leaders from diverse sectors. The symposium will foster collaboration and knowledge exchange, enabling attendees to enhance their skill sets and stay ahead in the rapidly evolving field of business continuity.

Upcoming Date **April 16, 2026** Toronto, ON

Les symposiums DRIC sont des événements d'une journée spécialement conçus pour les professionnels de haut niveau dans les domaines de la continuité des activités, de la reprise après sinistre, de la cyber-résilience et de la gestion des risques. Ils visent à fournir une plateforme dynamique et interactive permettant aux dirigeants d'explorer des stratégies innovantes, de partager les meilleures pratiques et de discuter des dernières tendances en matière de gestion de la continuité des activités.

Au cours de ces événements immersifs, les participants peuvent échanger avec des professionnels partageant les mêmes idées et des leaders d'opinion issus de divers secteurs. Le symposium favorisera la collaboration et l'échange de connaissances, permettant aux participants d'améliorer leurs compétences et de rester à la pointe dans le domaine en rapide évolution de la continuité des activités.

Prochaines date **16 avril 2026** Toronto, ON

CONTENTS • LE SOMMAIRE

* Click page number to navigate * Cliquez sur le numéro de page pour naviguer

Advertisers' Index • Index des annonceurs

Sponsor	Page	Website
Awards of Excellence	58	www.dri.ca/awards
Benoit Racette Services-conseils inc	50	racetteconseils.com
CRT/Demcon	35	crtdemcon.ca/crt/
DRIC - Upcoming Events	96	dri.ca/events.php
DRIC - Toronto Symposium (April 16)	2	www.dri.ca/one_day_symposiums.php
RIE Toronto	10	**drie.org/toronto**
Vanguard EMC Inc.	6	vanguardemergency.com

DRI CANADA Train. Prepare. Recover.
Former • Préparer • Rétablir

www.dri.ca

TRUE NORTH RESILIENCE
Résilience du vrai nord

DRI Canada's magazine / Magazine de DRI Canada

True North Resilience is published twice per year. Its mission is to facilitate the exchange of information among professionals in the field of disaster recovery, risk management, high availability and resilience; provide them with practical tools and techniques, and serve as a forum for discussion of emerging trends and issues.

La Magazine de Résilience du vrai nord est publié deux fois par an. Sa mission est de faciliter l'échange d'informations entre les professionnels dans le domaine de la reprise après sinistre, de la gestion des risques, de la haute disponibilité et de la résilience ; de leur fournir des outils et des techniques pratiques, et de servir de forum de discussion sur les tendances et les questions émergentes.

Manuscripts, other editorial submissions, and advertising should be submitted via email to:

Les manuscrits, les autres propositions éditoriales et la publicité doivent être envoyés par courrier électronique à l'adresse suivante:

Editor-in-Chief:
Garth Tucker, CBCP, CORP
Email: editors@dri.ca
Toll Free: 1-844-228-8135
Local: 416-646-2750

Send mailing list queries, and requests for reprints, bulk copies, or reprint permission by email to: editors@dri.ca, or by surface mail to:
DRIC, 701 Rossland Road East,
Suite 375, Whitby, ON, L1N 8Y9.

Envoyez vos demandes de renseignements sur la liste d'envoi et vos demandes de réimpression, de copies en vrac ou d'autorisation de réimpression par courriel à : editors@dri.ca, ou par courrier ordinaire à :
DRIC, 701 Rossland Road East,
Suite 375, Whitby, ON, L1N 8Y9.

Printed in Canada

About DRI Canada

DRI Canada is a non-profit organization that provides internationally recognized education and certification to business continuity, disaster recovery and emergency management professionals in Canada.

DRI CANADA mission (or how we are creating a value for our certified professionals):

- Promoting a base of common knowledge for the continuity and resiliency management profession together with DRI;
- Certifying qualified individuals in the disciplines of business continuity, disaster recovery and emergency management;
- Advocating for and increasing the professional value of DRI's credentials and those who hold them.

À propos de DRI Canada

DRI Canada est un organisme sans but lucratif qui offre une formation et une certification reconnues internationalement aux professionnels de la continuité des affaires, de la reprise après sinistre et de la gestion des urgences au Canada. Mission de DRI CANADA (ou comment nous créons une valeur pour nos professionnels certifiés) :

- Promouvoir une base de connaissances communes pour la profession de gestion de la continuité et de la résilience en collaboration avec DRI;
- Certifier des personnes qualifiées dans les disciplines de la continuité des affaires, de la reprise après sinistre et de la gestion des urgences;
- Promouvoir et accroître la valeur professionnelle des titres de compétences de DRI et de ceux qui les détiennent.

Graphic Design
Eclipse Technologies Inc.
416-219-8790
e-clipse.ca

Printing, Binding, Lettershop
Canmark Communicatrions
416.553.8228
canmarkcommunications.com

ISSN 2816-9018 (on-line)

President's Message
Message du président

By/Par Brenda Escribano, CBCP, President, DRI Canada

2026 marks the beginning of a new year and the start of a new Executive for the DRI Canada Board of Directors. True North Resilience continues to provide certified professionals with valuable insights into the world we all work in, while also offering an opportunity to spotlight the important work of your Board of Directors.

As your new President of the Board, I am thrilled to introduce our 2026 Executive. Together, we serve on your behalf to strengthen the resilience profession, advance our strategic priorities, and support the community of certified professionals across Canada.

Before welcoming the new Executive, I would like to extend heartfelt thanks to the 2025 Executive for their dedication, leadership, and service to you—our certified professionals.

2025 Executive

- President – Nancy HollowayWhite
- Vice President – Lisa Maddock
- Treasurer – Scott Leavitt
- Secretary/Privacy Officer – Brenda Escribano
- Past President – Brock Holowachuk

This group of individuals, alongside the full Board of Directors, helped shape the future of DRI Canada. Their work included updating the organization's strategic priorities and strengthening our foundation for the years ahead. We are deeply grateful for their commitment and contributions.

L'année 2026 marque le début d'une nouvelle année et l'entrée en fonction d'un nouveau comité exécutif au sein du conseil d'administration de DRI Canada. True North Resilience continue de fournir aux professionnels certifiés des informations précieuses sur le monde dans lequel nous travaillons tous, tout en offrant l'occasion de mettre en lumière le travail important de votre conseil d'administration.

En tant que nouveau président du conseil d'administration, je suis ravi de vous présenter notre équipe de direction pour 2026. Ensemble, nous travaillons en votre nom pour renforcer la profession de la résilience, faire progresser nos priorités stratégiques et soutenir la communauté des professionnels certifiés à travers le Canada.

Avant d'accueillir la nouvelle équipe de direction, je tiens à remercier chaleureusement l'équipe de direction 2025 pour son dévouement, son leadership et les services qu'elle a rendus à vous, nos professionnels certifiés.

Comité exécutif 2025

- Présidente – Nancy Holloway-White
- Vice-présidente – Lisa Maddock
- Trésorier – Scott Leavitt
- Secrétaire/Responsable de la protection de la vie privée – Brenda Escribano
- Ancien président – Brock Holowachuk

Ce groupe de personnes, aux côtés de l'ensemble du conseil d'administration, a contribué à façonner l'avenir de DRI Canada. Leur travail a consisté notamment à actualiser les priorités stratégiques de l'organisation et à renforcer nos fondations pour les années à venir. Nous leur sommes profondément reconnaissants pour leur engagement et leurs contributions.

With that, I am pleased to announce the 2026 Executive.

2026 Executive

- President – Brenda Escribano
- Vice President – Greg Solecki
- Treasurer – Scott Leavitt
- Secretary/Privacy Officer – Patrick Leduc
- Past President – Nancy HollowayWhite

"Thank you" hardly captures the appreciation we feel for the outgoing Executive. Now, let's learn a little more about your new Executive members.

Brenda Escribano, CBCP – President

Brenda Escribano, CBCP brings more than 25 years of experience in the Business Continuity Management (BCM) field within one of Canada's largest financial institutions. Her background spans both first and second lines of defense, and she has led diverse teams responsible for program execution,

Sur ce, j'ai le plaisir d'annoncer la composition de l'équipe de direction pour 2026.

Comité exécutif 2026

- Présidente – Brenda Escribano
- Vice-président – Greg Solecki
- Trésorier – Scott Leavitt
- Secrétaire/Responsable de la protection de la vie privée – Patrick Leduc
- Présidente sortante – Nancy Holloway-White

Un simple « merci » ne suffit pas à exprimer toute notre gratitude envers les membres sortants du comité exécutif. Découvrons maintenant un peu plus en détail les nouveaux membres du comité exécutif.

Brenda Escribano, CBCP – Présidente

Brenda Escribano

Brenda Escribano, CBCP, apporte plus de 25 ans d'expérience dans le domaine de la gestion de la continuité des activités (GCA) au sein de l'une des plus grandes institutions financières du Canada. Son expérience couvre à la fois les première et deuxième lignes de défense, et elle a dirigé diverses équipes chargées de l'exécution des programmes, de l'établissement de rapports et de la gestion des risques liés à la continuité des activités.

Plus récemment, Brenda a joué un rôle de premier plan dans une initiative pluriannuelle visant à passer d'une application BCM développée en interne à une nouvelle solution fournisseur à l'échelle de l'entreprise. Sa vaste expérience de la première ligne de défense dans de multiples segments d'activité lui confère une compréhension approfondie de la résilience opérationnelle et des risques organisationnels.

reporting, and business continuity risk management.

Most recently, Brenda played a key leadership role in a multiyear initiative to transition from a homegrown BCM application to a new enterprisewide vendor solution. Her extensive 1LoD experience across multiple business segments gives her a deep understanding of operational resilience and organizational risk.

Greg Solecki, MBCP, CEM – Vice President

A Master Business Continuity Professional whose career has been rooted in Canada's critical infrastructure framework, Greg has led continuity, preparedness, and recovery initiatives across aviation, public works, and Indigenous health while contributing to international crisis management standards. He is known for building and guiding high-performance teams under pressure, ensuring cohesive decision-making and resilient operations during rapidly evolving crises. As an experienced

facilitator and ICS instructor, Greg has supported every level of emergency management—from field operations to leading EOCs during some of Canada's largest disasters while advancing practical, risk-driven Business Impact Analyses across diverse organizations. Outside the EOC, he works with youth as a former Team Canada volleyball athlete, helping develop emerging players and strong communities.

Scott Leavitt, CBCP – Treasurer

Scott Leavitt, CBCP - Business Continuity and Disaster Recovery leader with 25+ years of experience directing continuity and resilience programs for industry-leading

Scott Leavit

Greg Solecki, MBCP, CEM – Vice-président

Greg Solecki

Professionnel chevronné de la continuité des activités dont la carrière est ancrée dans le cadre des infrastructures essentielles du Canada, Greg a dirigé des initiatives de continuité, de préparation et de reprise dans les domaines de l'aviation, des travaux publics et de la santé des Autochtones, tout en contribuant à l'élaboration de normes internationales en matière de gestion de crise. Il est connu pour sa capacité à constituer et à diriger des équipes hautement performantes sous pression, en garantissant une prise de décision cohérente et des opérations résilientes lors de crises en évolution rapide. En tant que facilitateur expérimenté

facilitateur et formateur ICS expérimenté, Greg a apporté son soutien à tous les niveaux de la gestion des urgences, des opérations sur le terrain à la direction des COU lors de certaines des plus grandes catastrophes au Canada, tout en faisant progresser les analyses d'impact sur les activités pratiques et axées sur les risques dans diverses organisations. En dehors du COU, il travaille avec les jeunes en tant qu'ancien athlète de l'équipe canadienne de volley-ball, aidant à former de nouveaux joueurs et à renforcer les communautés.

Scott Leavitt, CBCP – Trésorier

Scott Leavitt, CBCP - Responsable de la continuité des activités et de la reprise après sinistre, avec plus de 25 ans d'expérience dans la direction de programmes de continuité et de résilience pour des organisations leaders dans leur secteur. Reconnu pour avoir accompagné des équipes de direction lors d'incidents et de crises majeurs, et pour avoir mis en place des solutions de continuité

organizations. Known for coaching executive teams through major incidents and crises, and for building practical, testable continuity solutions that strengthen operational readiness. Brings deep expertise in IT high availability and disaster recovery as a consultant and subject-matter expert, leading program design, delivery, and end-to-end testing. Thrives in fast-paced environments, balancing competing priorities while working autonomously with discretion and sound judgment.

Patrick Leduc, CBCP – Secretary/Privacy Officer

Patrick Leduc

Mr. Patrick Leduc, CBCP, is a bilingual Risk Management and Organizational Resilience Consultant with more than 25 years of experience in business continuity, emergency management, crisis governance, and operational risk.

He specializes in designing and leading endtoend BCM programs—from strategic governance frameworks to operational execution. Patrick has supported organizations operating in complex, highrisk environments, including healthcare systems, municipalities, and government agencies.

His experience includes key roles in major crisis responses such as the COVID19 pandemic and the LacMégantic train derailment. Known for bridging strategy and execution, Patrick delivers practical, compliant, and sustainable resilience solutions aligned with legal, regulatory, and industry best practices, while staying engaged with emerging trends in the resilience field.

pratiques et testables qui renforcent la préparation opérationnelle. Il apporte une expertise approfondie en matière de haute disponibilité informatique et de reprise après sinistre en tant que consultant et expert en la matière, dirigeant la conception, la mise en œuvre et les tests de bout en bout des programmes. Il excelle dans les environnements d' s en évolution rapide, équilibrant les priorités concurrentes tout en travaillant de manière autonome avec discrétion et bon sens.

Patrick Leduc, CBCP – Secrétaire/ Responsable de la protection de la vie privée

M. Patrick Leduc, CBCP, est un consultant bilingue en gestion des risques et en résilience organisationnelle qui compte plus de 25 ans d'expérience dans les domaines de la continuité des activités, de la gestion des urgences, de la gouvernance de crise et des risques opérationnels.

Il est spécialisé dans la conception et la direction de programmes de gestion de la continuité des activités de bout en bout, depuis les cadres de gouvernance stratégique jusqu'à l'exécution opérationnelle. Patrick a aidé des organisations opérant dans des environnements complexes et à haut risque, notamment des systèmes de santé, des municipalités et des agences gouvernementales.

Il a notamment joué un rôle clé dans la gestion de crises majeures telles que la pandémie de COVID-19 et le déraillement ferroviaire de Lac-Mégantic. Reconnu pour sa capacité à faire le lien entre la stratégie et l'exécution, Patrick propose des solutions de résilience pratiques, conformes et durables, alignées sur les meilleures pratiques juridiques, réglementaires et industrielles, tout en restant à l'affût des nouvelles tendances dans le domaine de la résilience.

Nancy HollowayWhite – Past President, CBCP, CBCA


Nancy Holloway-White

Nancy Holloway-White, CBCP, CBCA is a Director in financial services risk management with more than 15 years of experience across the corporate sector, having led teams in operations and risk management in financial services and insurance. Her professional focus combines risk management, process effectiveness, controls, and change management. She holds the CBCP and CBCA certifications from DRI and is deeply committed to advancing the business continuity profession. A life-long volunteer, Nancy has contributed more than a decade of service to DRI Canada, serving in numerous leadership roles including Chair of the Education Commission, Chair of the Online Learning Steering Committee, Vice President, and until recently President of the DRI Canada Board of Directors. She has also served six years on a community board, concluding her term as President, and is passionate about mentoring, philanthropy, and supporting students transitioning into the workforce.

Nancy has spoken at the Continuity & Resilience Today conference and DRI Canada symposiums and has received multiple awards recognizing her leadership and volunteer contributions, including the DRI Canada Builder Award and Board of Directors Achievement Award. During her recent board terms, she has played a key role in DRI Canada's strategic planning, focusing on increased engagement, outreach, and participation across the profession. Outside of work, Nancy enjoys spending time with family and friends, and being outdoors.

Please join me in thanking the outgoing Executive and congratulating the 2026 Executive of the DRI Canada Board of Directors. I look forward to the year ahead and to continuing our shared commitment to advancing resilience across Canada. Ω

Nancy Holloway-White – Ancienne présidente, CBCP, CBCA

Nancy Holloway-White, CBCP, CBCA est directrice de la gestion des risques dans le secteur des services financiers. Elle possède plus de 15 ans d'expérience dans le secteur des entreprises, ayant dirigé des équipes dans les domaines des opérations et de la gestion des risques dans les services financiers et les assurances. Son expertise professionnelle combine la gestion des risques, l'efficacité des processus, les contrôles et la gestion du changement. Elle est titulaire des certifications CBCP et CBCA de DRI et est profondément engagée dans la promotion de la profession de la continuité des activités. Bénévole de longue date, Nancy a consacré plus d'une décennie au service de DRI Canada, occupant de nombreux postes de direction, notamment ceux de présidente de la commission de l'éducation, de présidente du comité directeur de l'apprentissage en ligne, de vice-présidente et, jusqu'à récemment, de présidente du conseil d'administration de DRI Canada. Elle a également siégé pendant six ans à un conseil communautaire, où elle a terminé son mandat de présidente, et se passionne pour le mentorat, la philanthropie et le soutien aux étudiants en transition vers le marché du travail.

Nancy a pris la parole lors de la conférence Continuity & Resilience Today et des symposiums de DRI Canada. Elle a reçu de nombreux prix reconnaissant son leadership et ses contributions bénévoles, notamment le prix Builder Award et le prix Board of Directors Achievement Award de DRI Canada. Au cours de ses récents mandats au conseil d'administration, elle a joué un rôle clé dans la planification stratégique de DRI Canada, en mettant l'accent sur l'engagement, la sensibilisation et la participation accrus à l› e de la profession. En dehors du travail, Nancy aime passer du temps avec sa famille et ses amis, et être à l'extérieur.

Je vous invite à vous joindre à moi pour remercier les membres sortants du conseil d'administration et féliciter les membres du conseil d'administration de DRI Canada pour 2026. Je me réjouis à l'idée de poursuivre notre engagement commun en faveur de la résilience à travers le Canada au cours de l'année à venir. Ω

Your Network for Resilience. Your Community of Practice.

RIE Toronto is more than a professional association — it's a networking community where business continuity, disaster recovery, emergency management, and crisis management and other resilence professionals connect, learn from each other, and build lasting professional relationships.

Founded in 1985 and part of a national and chapter network, RIE provides the kind of peer-to-peer connections you can't get from a conference alone. Our events are practitioner-driven, vendor-neutral, and designed to foster real conversation between people doing this work every day.

2026 is shaping up to be our strongest year yet. We kicked off with an *Ask RIE Anything* webinar featuring risk & resilience expert Mike Janko (MBCP, MBCI, ARM, CBCLA, CEOE), followed by a hands-on eBRP crisis simulation workshop. Later in Q2, we're hosting a *Cyber Resilience Symposium* with expert speakers, and a practitioner roundtable. We're also exploring new initiatives including a *Lunch & Learn Workshop Series* in collaboration with our sponsors and the revival of the *Mentorship Program*, pairing experienced practitioners with emerging professionals in the field.

Why Join? Membership gives you access to quarterly webinars and in-person symposiums, continuing education credits toward CFCP, CBCP, and MBCP certifications, free participation in events across all RIE chapters, archived presentations from past sessions, conference discounts through partner organizations, and – most importantly – a growing network of resilience professionals who understand the challenges you face.

Ready to Join? Sign up at drie.org/toronto - Join Now

Votre réseau pour la résilience. Votre communauté de pratique.

RIE Toronto est plus qu'une association professionnelle, c'est une communauté de réseautage où les professionnels de la continuité des activités, de la reprise après sinistre, de la gestion des urgences et de la gestion des crises, ainsi que d'autres professionnels de la résilience se rencontrent, apprennent les uns des autres et établissent des relations professionnelles durables.

Fondée en 1985 et faisant partie d'un réseau national et régional, RIE offre le type de relations entre pairs que vous ne pouvez pas obtenir lors d'une simple conférence. Nos événements sont axés sur les praticiens, neutres vis-à-vis des fournisseurs et conçus pour favoriser de véritables conversations entre les personnes qui exercent ce métier au quotidien.

2026 s'annonce comme notre meilleure année à ce jour. Nous avons commencé par un webinaire *«Demandez tout à RIE»* avec Mike Janko (MBCP, MBCI, ARM, CBCLA, CEOE), expert en risques et résilience, suivi d'un atelier pratique de simulation de crise eBRP. Plus tard au deuxième trimestre, nous organiserons un *symposium sur la cyber-résilience* avec des conférenciers experts et une table ronde de praticiens. Nous explorons également de nouvelles initiatives, notamment *une série d'ateliers « Lunch & Learn »* en collaboration avec nos sponsors et la relance du *programme de mentorat*, qui met en relation des praticiens expérimentés avec des professionnels émergents dans le domaine.

Pourquoi adhérer ? L'adhésion vous donne accès à des webinaires trimestriels et à des symposiums en personne, à des crédits de formation continue pour les certifications CFCP, CBCP et MBCP, à la participation gratuite à des événements dans toutes les sections RIE, aux présentations archivées des sessions précédentes, à des réductions sur les conférences par l'intermédiaire d'organisations partenaires et, surtout, à un réseau croissant de professionnels de la résilience qui comprennent les défis auxquels vous êtes confrontés.

Prêt à vous inscrire ? Inscrivez-vous sur drie.org/toronto – Inscrivez-vous dès maintenant

Editors' Desk
Bureau des rédacteurs

This is the 8th issue of True North Resilience – Four years!

That really feels unbelievable because it seems like a week ago the idea was first pitched to the DRI Canada Board of Directors in Nov 2020. Time flies when you're having fun, and while putting the magazine together can be stressful (think four authors ghosting you less than a month before the deadline – so basically 4/5ths of the planned edition), it's worth it in the end. Keep in mind that almost everyone (98%) involved is a volunteer, from the editors on the review committee, to the Board members that make up the steering committee, and most importantly, the authors!

This issue we have a new feature that came about, like most great ideas, as a spur of the moment thought that everyone agreed was a great idea, and it is now a thing - Letters to the Editor! For each issue going forward, we encourage you to submit your comment(s) on a resilience related subject or event. Please keep the content professional but thought provoking. Thanks to **Alexander Landry** for suggesting it based on his review of **Kevin Powers'** article, "Old Man Yells at Cloud." We hope you enjoy this new feature as much as we do.

This issue we have some great articles from new TNR authors and a couple from old friends of the magazine. The cover story, by **Eric Corriveau**, is a look into the

Voici le8enuméro de True North Resilience – Quatre ans!

Cela semble vraiment incroyable, car il y a à peine une semaine, l'idée a été présentée pour la première fois au conseil d'administration de DRI Canada en novembre 2020. Le temps passe vite quand on s'amuse, et même si la préparation du magazine peut être stressante (imaginez quatre auteurs qui vous ignorent moins d'un mois avant la date limite, soit pratiquement les quatre cinquièmes de l'édition prévue), cela en vaut la peine au final. N'oubliez pas que presque toutes les personnes impliquées (98%) sont des bénévoles, des rédacteurs du comité de révision aux membres du conseil d'administration qui composent le comité directeur, sans oublier les auteurs !

Dans ce numéro, nous proposons une nouvelle rubrique qui, comme la plupart des bonnes idées, est née d'une impulsion du moment que tout le monde a trouvée excellente, et qui est désormais une réalité. Lettres à la rédaction ! Pour chaque numéro à venir, nous vous encourageons à nous envoyer vos commentaires sur un sujet ou un événement lié à la résilience. Veuillez veiller à ce que le contenu soit professionnel, mais suscite la réflexion. Merci à **Alexander Landry** de l'avoir suggérée après avoir lu l'article de **Kevin Powers**, « Old Man Yells at Cloud ». Nous espérons que vous apprécierez cette nouvelle rubrique autant que nous.

recent exercise by Montfort, Ontario's French-language university hospital, in collaboration with the Ottawa Police Service – "Code Argent Simulation". Very well developed and executed exercise all around and will certainly help with your exercise program (DRI PP#8). It also ties in with DRIC's "Year of the Exercise". 2026's focus is on exercises, and you can find the kick off to "DRIC's Amazing Canadian Exercise" later in the magazine. Something that all of us are pretty excited about: Get a team together and "Come on down! These prizes can be yours if the responses are right!" (Yes, cheesy Price is Right reference… Did I mention we're all volunteers?)

As always, we hope you enjoy the magazine and get useful direction for your programs!

The TNR Editorial Review Committee

- Ron Andrews
- Brady Podloski
- Alexander Landry
- Garth Tucker
- Charlie Karle

P.S. If you wish to get involved with the Editorial Review Committee as a volunteer editor to review articles for content and grammar, please forward your experience to editors@dri.ca. Thanks!

- Garth Ω

Dans ce numéro, nous vous proposons d'excellents articles rédigés par de nouveaux auteurs de TNR et quelques-uns par de vieux amis du magazine. L'article à la une, signé **Eric Corriveau**, porte sur l'exercice récemment mené par l'hôpital universitaire francophone de Montfort, en Ontario, en collaboration avec le Service de police d'Ottawa : « Code Argent Simulation ». Cet exercice, très bien conçu et exécuté, vous aidera certainement dans votre programme d'exercices (DRI PP#8). Il s'inscrit également dans le cadre de l'« Année de l'exercice » du DRIC. L'année 2026 sera axée sur les exercices, et vous trouverez plus loin dans le magazine le coup d'envoi de « DRIC's Amazing Canadian Exercise ». Quelque chose qui nous enthousiasme tous : formez une équipe et « Venez nombreux ! Ces prix peuvent être à vous si vous répondez correctement ! » (Oui, c'est une référence un peu kitsch à The Price is Right... Ai-je mentionné que nous sommes tous bénévoles ?)

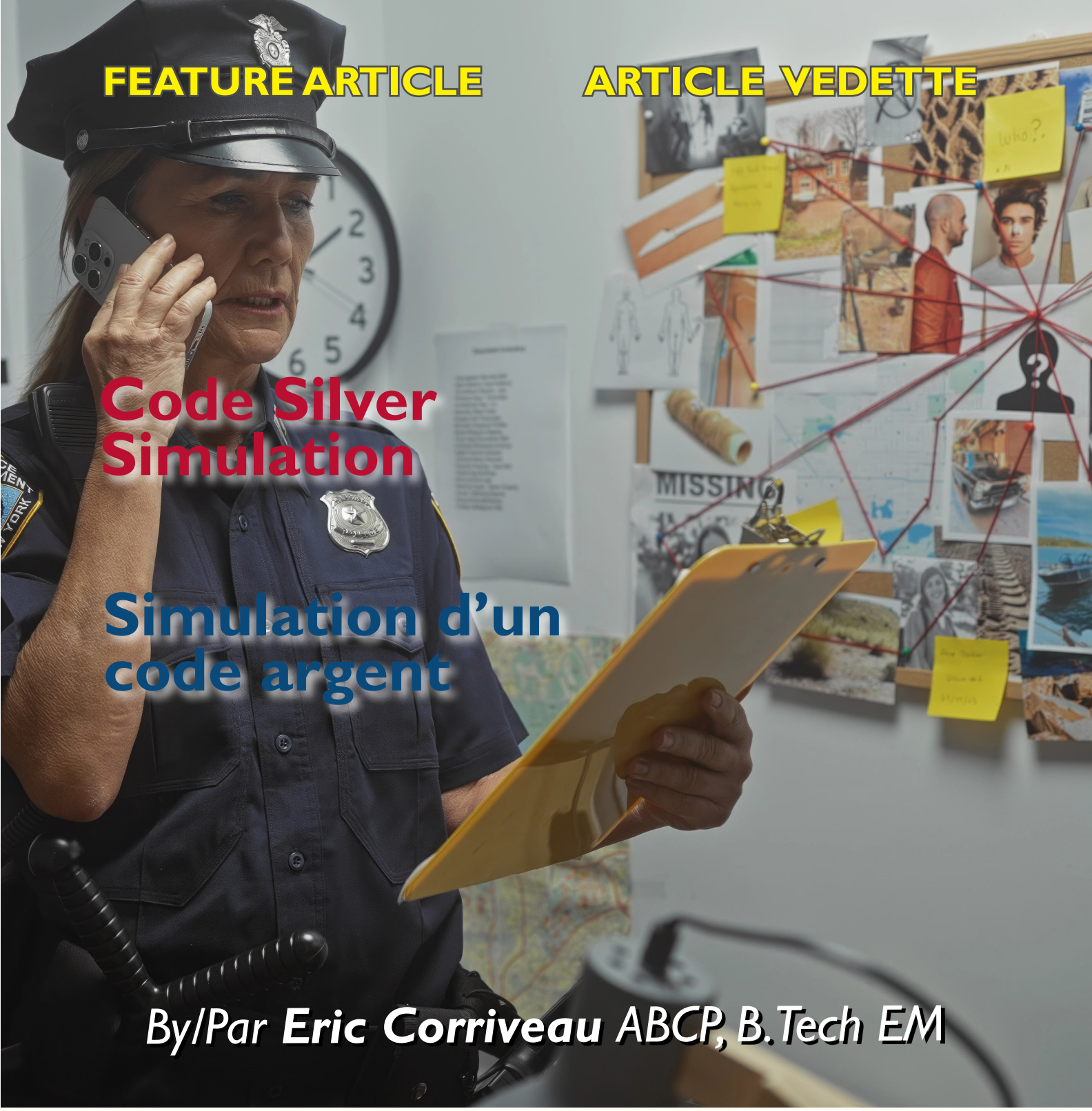
Comme toujours, nous espérons que vous apprécierez le magazine et que vous y trouverez des conseils utiles pour vos programmes !

Le comité de révision éditoriale de TNR

- Ron Andrews
- Brady Podloski
- Alexander Landry
- Garth Tucker
- Charlie Karle

P.S. Si vous souhaitez vous impliquer dans le comité de révision éditoriale en tant que rédacteur bénévole chargé de réviser le contenu et la grammaire des articles, veuillez envoyer votre CV àeditors@dri.ca. Merci !

- Garth Ω



Editor's note

Code Silver is an emergency signal used in hospitals and institutions to indicate the presence of an active shooter, an armed person, or an imminent armed threat. It triggers immediate lockdown: barricade yourself in a room, turn off the lights, remain silent, and call 911.

Note de la rédaction

Le code Argent est un signal d'urgence utilisé dans les hôpitaux et institutions pour indiquer la présence d'un tireur actif, d'une personne armée ou d'une menace armée imminente. Il déclenche le confinement immédiat : barricadez-vous dans un local, éteignez les lumières, restez silencieux et appelez le 911.

Code Silver simulation

Armed individual in hospital: simulation to save lives
When collective learning strengthens the response

Date: December 2025

Summary:

This study presents a Code Silver simulation conducted at Montfort, Ontario's French-language university hospital, in collaboration with the Ottawa Police Service, to assess the organization's preparedness for an armed threat. The scenario, inspired by real incidents, included a hostage situation and several critical inputs such as media pressure, clinical deterioration, cardiac arrest, competing calls, and social media activity. The 60-minute exercise mobilized the Incident Management System (IMS), operational sub-simulations, and an operational risk assessment (ORA) based on recognized standards. The results highlighted significant strengths, including interdisciplinary coordination, as well as opportunities for improvement in certain aspects of communications, police-security liaison, gradual deconfinement, and control center management. Police officers were able to adapt their protocols to a complex hospital environment. The lessons learned were translated into measurable capabilities using the Operational Risk Assessment (ORA), Hazard Risk Vulnerability Analysis (HRVA)/ Hazard Identification and Risk Assessment (HIRA), Plan-Do-Check-Act (PDCA), and the Personal Health Information Protection Act, Ontario (PHIPA), strengthening hospital resilience.

Keywords: *Armed individual; silver code; SGI/ IMS; unified command; lockdown; PHIPA; HRVA/ HIRA; PCA; RAVE; communications; continuity of care.*

Simulation de le Code Argent

Individu armé à l'hôpital : simuler pour sauver
Quand l'apprentissage collectif renforce la réponse

Date : Décembre 2025

Résumé :

Cette étude présente une simulation de Code argent réalisée à Montfort, l'hôpital universitaire francophone de l'Ontario, en collaboration avec le Service de police d'Ottawa, visant à évaluer la préparation de l'organisation face à une menace armée. Le scénario, inspiré d'incidents réels, incluait une prise d'otage et plusieurs intrants critiques tels que : pression médiatique, détérioration clinique, arrêt cardiaque, appels concurrents et activités sur les médias sociaux. L'exercice, d'une durée de 60 minutes, a mobilisé la structure de gestion des incidents (SGI) (Incident Management System [IMS]), des sous-simulations opérationnelles et une évaluation des risques opérationnels (ERO) fondée sur des normes reconnues. Les résultats ont mis en évidence des forces importantes, notamment la coordination interdisciplinaire, ainsi que des opportunités d'amélioration quant à certains aspects des communications, de la liaison police-sécurité, de déconfinement progressif et de gestion du centre de contrôle. Les policiers ont pu adapter leurs protocoles à un environnement hospitalier complexe. Les enseignements tirés ont été traduits en capacités mesurables via les outils Évaluation des risques opérationnels (ERO), Hazard Risk Vulnerability Analysis (HRVA)/Hazard Identification and Risk Assessment (HIRA), Planifier – Exécuter – Vérifier – Agir (PDCA) et Loi sur la protection des renseignements médicaux de l'Ontario, Loi sur la protection des renseignements médicaux de l'Ontario (PHIPA), renforçant la résilience hospitalière.

Organizational context

Prior to the exercise, the institution had a Silver Code policy and lockdown procedures in place, a mobilizable SGI structure, emergency communication methods (intercom, radio, etc.), and messages that could be used in emergency situations. In addition, staff members are required to review the Silver Code procedure annually and participate in a skills maintenance exercise, whether tabletop or functional, to recreate the application of lockdown protocols and expected actions under realistic conditions.

Objectives: measure the maturity of the plans and systems in place; evaluate the management unit, police-security liaison, and protected channels; test communications and messages; ensure continuity of care and operations; standardize PHIPA decisions.

Methods

Organizational simulation case study (Code Silver) with actors moving within the organization, qualitative analysis and normative mapping (CSA Z1600/HSO 9002), targeting a PDCA plan and indicators (KPIs). Two SGI sub-simulations densified the simulation inputs (communications, flows, PHIPA, continuity) within the main framework.

Evaluation and scenario governance (accuracy)

In order to minimize the impact on the hospital user experience, all clinical and administrative sectors (1) under pressure conducted a ten-minute tabletop exercise organized by the manager or person in charge of the sector. They had to indicate in a written report what they would do at that time of day with the number of staff, patients, and visitors present and according to their disposition at the time of the initial call. A subsequent review was planned with the sectors to review their actions and decisions. For sectors that were in regular occupancy (2), an actual lockdown with movement of staff and patients was carried out, with a written report similar to that of group (1).

To monitor the situation of the armed individual (3), the security manager observed the maneuver with a police evaluator/educator to assess the protocols in place on both the police and hospital sides. A report following the simulation was written on the unfolding of the situation, as well as the lessons learned and areas for improvement for each party.

Mots-clés : *Individu armé ; code argent ; SGI/IMS ; commande unifiée ; confinement (Lockdown) ; PHIPA ; HRVA/HIRA ; PCA ; RAVE ; communications ; continuité des soins.*

Contexte organisationnel

Avant l'exercice, l'établissement disposait d'une politique de Code argent et de procédures de confinement (lockdown), d'une structure SGI mobilisable, de moyens de communication en cas d'urgence (interphone, radio, etc.), et de messages pouvant être utilisés lors de situations d'urgence. De plus, les membres du personnel ont l'obligation de revoir annuellement la procédure de Code argent et de participer à un exercice de maintien des compétences, qu'il s'agisse d'un exercice de type tabletop ou fonctionnel, afin de recréer en conditions réalistes l'application des protocoles de confinement et des actions attendues.

Objectifs : mesurer la maturité des plans et dispositifs en place ; évaluer la cellule de gestion ainsi que la liaison police-sécurité et les voies/canaux protégés ; tester les communications et les messages ; assurer la continuité des soins et des opérations ; uniformiser la décision PHIPA.

Méthodes

Étude de cas de simulation organisationnelle (Code argent) avec des acteurs se déplaçant dans l'organisation, analyse qualitative et cartographie normative (CSA Z1600/HSO 9002), visant un plan PDCA et des indicateurs (KPI). Deux sous-simulations SGI ont densifié les intrants de la simulation (communications, flux, PHIPA, continuité) à l'intérieur de la trame principale.

Gouvernance de l'évaluation et du scénario (précision)

Dans le but de diminuer l'impact sur l'expérience des usagers de l'hôpital, tous les secteurs cliniques et administratifs (1) sous pression ont effectué un exercice théorique de type tabletop de dix minutes

To monitor the SGI unit (4), a specialist and instructor from the SGI structure measured and evaluated the objectives, frequency of updates, interdepartmental coordination, and decisions made by the crisis unit. All decisions were recorded for a post-activity report (AAR).

Scenario and input architecture

The scenario architecture was based on real events from incident reports that demonstrated a risk of escalation. A critical variable was incorporated, leading to a dangerous situation involving an armed individual and a hostage situation. To ensure maximum realism, the 60-minute simulation was conducted in collaboration with the Ottawa Police Service: a police trainer played the role of the attacker, while negotiators and trainees played the roles of responders.

After this initial scenario, the team revisited the actions related to triggering a Code Silver. Once the protocol was activated and the crisis unit was opened, various operational inputs were added to test the robustness of the plans and increase the pressure to make decisions, with the goal of maximizing learning.

Depending on the needs of the scenario, additional critical events were incorporated: media pressure, targeted evacuation, clinical deterioration of a patient, cardiac arrest, simultaneous emergency calls, and social

organisées par le gestionnaire ou une personne responsable du secteur. Ils durent indiquer sur un rapport écrit ce qu'ils feraient à ce moment de la journée avec le nombre de membres du personnel, patients et visiteurs présents et selon la disposition de ceux-ci lors de l'appel initial. Une révision subséquente fut planifiée avec les secteurs pour une revue de leurs actions et décisions. Pour les secteurs qui étaient en occupation régulière (2), un verrouillage réel avec mouvement du personnel et des patients fut effectué, avec rapport écrit du même type que le groupe (1).

Pour le suivi de la situation de l'individu armé (3), le gestionnaire de la sécurité a observé la manœuvre avec un policier évaluateur/éducateur pour évaluer les protocoles en places tant du côté des policiers que de l'hôpital. Un rapport suite à la simulation fut écrit sur le déroulement de la situation ainsi que les leçons apprises et le point d'amélioration à apporter pour chaque partie.

Pour le suivi de la cellule SGI (4), un spécialiste et enseignant de la structure SGI a mesuré et évalué les objectifs, la cadence des mises à jour, la coordination interservices et les décisions prises par la cellule de crise. Toutes les décisions ont été consignées pour un rapport post-activité (AAR).

Scénario et architecture des intrants

L'architecture du scénario s'appuyait sur des événements réels issus de rapports d'incidents ayant démontré un risque de dégénérescence. Une variable critique y a été intégrée, menant à une situation dangereuse évoluant vers la présence d'une personne armée et une prise d'otage. Pour assurer un réalisme maximal, la simulation de 60 minutes a été réalisée en collaboration avec le Service de police d'Ottawa : un policier formateur incarnait l'agresseur, tandis que des négociateurs et des agents en formation jouaient les intervenants.

Après cette trame initiale, l'équipe a revisité les actions liées au déclenchement d'un

media posts. External partners were also simulated by telephone, in particular to report behavior deemed suspicious.

The simulation was based on the resources actually available at the time of the trigger: the severity of the sectors, the staff present, and the weather conditions in November. Staff were informed seven days in advance, with reminders sent out afterwards.

Posters and messages on televisions announced the exercise to patients and visitors. The attacker and supervisors wore red bibs. Before the start, an information round was conducted, specifying that screams or noises could occur without ever involving patients or staff. During the movements, supervisors opened and closed the passageway using "simulation in progress" signs to avoid panic and warn people in the areas being crossed.

Results

In order to rigorously evaluate the effectiveness of the simulation, we conducted a survey of all participants before and after the simulation. This allowed us to collect both qualitative and quantitative data on their knowledge, perceptions, and level of preparedness. The questionnaires also sought detailed feedback on the relevance of the simulation, the achievement of operational objectives, and the clarity of roles and responsibilities in an emergency situation.

This methodological approach provided an accurate picture of the real impact of the simulation, particularly with regard to participants' ability to apply the procedure, effectively assume their roles, and make informed decisions in an emergency context. The comments collected also identified concrete areas for improvement in order to optimize future simulations and strengthen organizational preparedness.

The exercise highlighted various opportunities for improvement. First, certain gaps were identified in some aspects of

Code argent. Une fois le protocole activé et la cellule de crise ouverte, divers intrants opérationnels ont été ajoutés pour éprouver la robustesse des plans et accroître la pression décisionnelle, dans un objectif d'apprentissage maximal.

Selon les besoins du scénario, des événements critiques supplémentaires ont été intégrés : pressions médiatiques, évacuation ciblée, aggravation clinique d'un patient, arrêt cardiaque, appels d'urgence simultanés et publications sur les médias sociaux. Des partenaires externes ont aussi été simulés par téléphone, notamment pour signaler des comportements jugés suspects.

La simulation reposait sur les ressources réellement disponibles au moment du déclenchement : acuité des secteurs, effectifs présents et conditions météorologiques de novembre. Le personnel avait été informé sept jours avant, avec rappels transmis par la suite.

Pour les patients et visiteurs, des affiches et messages sur les téléviseurs annonçaient l'exercice. L'agresseur et les surveillants portaient des dossards rouges. Avant le début, une ronde d'information a été faite, précisant que des cris ou bruits pourraient survenir sans jamais impliquer les patients ou le personnel. Durant les déplacements, les surveillants ouvraient et fermaient le passage à l'aide de panneaux « simulation en cours » afin d'éviter la panique et de prévenir les personnes dans les secteurs traversés.

Résultats

Afin d'évaluer de manière rigoureuse l'efficacité de la simulation, nous avons administré un sondage auprès de l'ensemble des participants, avant et après la simulation. Cette démarche nous a permis de recueillir des données à la fois qualitatives et quantitatives sur leurs connaissances, leurs perceptions et leur niveau de préparation. Les questionnaires visaient également à obtenir une rétroaction détaillée concernant la pertinence de la simulation, l'atteinte des

the communications and liaison roles. For example, a clear link should be established between the control center and police services, both for operational issues and liaison needs, as well as to validate external communications. In addition, staff and partner s would have appreciated receiving more frequent updates on the status of the situation.

The deconfinement process must be applied in a targeted and gradual manner, one sector at a time, to avoid reopening areas that remain at risk. It is also essential to quickly direct patients who are already outside the facility to a safe location.

The exercise also highlighted the need for a better distribution of responsibilities within the security team. The shift supervisor must devote himself entirely to managing the emergency situation in collaboration with the police, while the security coordinator will take charge of the continuity of operations for the entire facility. This separation reduces the workload of the security manager and improves the overall effectiveness of the response.

Finally, the security control center must be relocated to a backup location in another area of the hospital. This approach optimizes communication between police officers and senior management, while ensuring a safe environment for staff members.

For the police, the exercise provided a unique opportunity to train in an unconventional environment, very different from the usual context of intervention. This immersion in a hospital setting made it possible to test and refine response protocols adapted to healthcare facilities, where the high density of patients, visitors, and staff considerably complicates operational management.

objectifs opérationnels ainsi que la clarté des rôles et responsabilités en situation d'urgence.

Cette approche méthodologique a offert un portrait précis de l'impact réel de la simulation, notamment en ce qui concerne la capacité des participants à appliquer la procédure, à assumer efficacement leur rôle et à prendre des décisions éclairées dans un contexte d'urgence. Les commentaires recueillis ont aussi permis d'identifier des pistes d'amélioration concrètes afin d'optimiser les simulations futures et de renforcer la préparation organisationnelle.

L'exercice a permis de mettre en lumière diverses opportunités d'amélioration. D'abord, certaines lacunes ont été identifiées quant à certains aspects des rôles responsables des communications et de la liaison. Par exemple, un lien devrait être clairement établi entre le centre de contrôle et les services policiers, tant pour des questions opérationnelles que pour des besoins de liaison, ou encore pour valider les communications externes. De plus, des membres du personnel et des partenaires auraient apprécié recevoir des mises à jour plus fréquemment quant à l'état de la situation.

Le processus de déconfinement doit être appliqué de façon ciblée et progressive, un secteur à la fois, afin d'éviter la réouverture de zones demeurant à risque. Il est également essentiel d'orienter rapidement les patients déjà à l'extérieur de l'établissement vers un lieu sécuritaire.

L'exercice a aussi mis en évidence la nécessité de mieux répartir les responsabilités au sein de l'équipe de sécurité. Le responsable de quart doit se consacrer entièrement à la gestion de la situation d'urgence en collaboration avec les policiers, tandis que le coordonnateur de la sécurité prendra en charge la continuité des opérations pour l'ensemble de l'établissement. Cette séparation permet de réduire la charge de travail du responsable de la sécurité et d'améliorer l'efficacité globale de la réponse.

Enfin, le centre de contrôle de la sécurité doit être relocalisé en mode « backup » dans un autre secteur de l'hôpital. Cette approche permet d'optimiser les échanges entre les policiers et la haute direction, tout en assurant un environnement sécuritaire pour les membres du personnel.

Police officers were also able to educate and train staff on the expected behaviors during an intervention involving an armed person in a high-risk area. The hospital environment presents additional dangers, including the presence of medical oxygen, radiology equipment, combustible sources, and confined spaces, which require close coordination and rigorous application of procedures.

The exercise generated significant value for both organizations: police officers were able to refine their approach in a real hospital setting, while staff benefited from practical training with specialized responders. The lessons learned from this collaboration strengthened mutual understanding of the risks and the complementary nature of their roles in critical situations. Both parties expressed a sincere interest in repeating the experience, either on the same theme or in different scenarios, in order to continue improving their joint preparedness.

Business Continuity Plan (BCP)

To ensure business continuity during the armed individual simulation, we applied a structured approach based on identifying critical services and protecting essential activities. Targeted containment and the establishment of protected routes made it possible to secure sensitive areas while maintaining priority care. Staff redeployment and the maintenance of support

Du côté policier, l'exercice a offert une occasion unique de s'entraîner dans un environnement non conventionnel, très différent du contexte d'intervention habituel. Cette immersion en milieu hospitalier a permis de mettre à l'épreuve et de raffiner les protocoles de réponse adaptés aux infrastructures de santé, où la forte densité de patients, visiteurs et membres du personnel complexifie considérablement la gestion opérationnelle. Les policiers ont également pu sensibiliser et former le personnel présent aux comportements attendus lors d'une intervention impliquant une personne armée dans un secteur à haut risque. L'environnement hospitalier comporte en effet des dangers supplémentaires, notamment la présence d'oxygène médical, d'équipements de radiologie, de sources combustibles et d'espaces confinés, ce qui exige une coordination étroite et une application rigoureuse des procédures.

L'exercice a généré une valeur importante pour les deux organisations : les policiers ont pu perfectionner leur approche en contexte hospitalier réel, tandis que le personnel a bénéficié d'un entraînement pratique avec des intervenants spécialisés. Les apprentissages issus de cette collaboration ont renforcé la compréhension mutuelle des risques et la complémentarité des rôles en situation critique. Les deux parties ont d'ailleurs exprimé un intérêt sincère à renouveler l'expérience, que ce soit sur la même thématique ou dans le cadre de scénarios différents afin de poursuivre l'amélioration continue de leur préparation commune.

Plan de continuité des activités (PCA)

Pour assurer la continuité des activités lors de la simulation d'un individu armé, nous avons appliqué une approche structurée fondée sur l'identification des services critiques et la protection des activités essentielles. Le confinement ciblé et la mise en place de voies protégées ont permis de sécuriser les zones sensibles tout en maintenant les soins prioritaires. Le redéploiement

functions (logistics, communications, supplies) were planned to limit disruptions. Fallback areas and off-site accommodation options were identified to ensure the safety of patients and staff. Communications were centralized and simplified to ensure clarity of instructions. Finally, the post-incident recovery phase incorporated performance indicators such as service uptime, percentage of protected circuits, recovery times, number of interruptions, and stakeholder satisfaction.

Limitations and next steps

This was the first exercise conducted jointly with the police department. To minimize the impact on patients, only a quick exercise was required for clinical staff under pressure, without resorting to total lockdown. A few weeks after the simulation, a survey was sent to staff to obtain a qualitative and quantitative view of the simulation in order to measure, analyze, and subsequently compare the results obtained during a future joint exercise. The next steps will be to share the lessons learned with hospitals in the region and the police department to improve cooperation and the safety of our services. Updating our

du personnel et le maintien des fonctions de support (logistique, communications, approvisionnement) ont été planifiés pour limiter les interruptions. Des zones de repli et des options d'hébergement hors site ont été définies pour garantir la sécurité des patients et du personnel. Les communications ont été centralisées et simplifiées afin d'assurer la clarté des directives. Enfin, la phase de rétablissement post-incident a intégré des indicateurs de performance, tels que le temps de maintien des services, le pourcentage de circuits protégés, les délais de reprise, le nombre d'interruptions et la satisfaction des parties prenantes.

Limites et prochaines étapes

Cet exercice fut le premier mené conjointement avec le service de police. Pour diminuer l'impact aux patients, seul un exercice rapide était demandé pour le personnel clinique sous pression sans recourir au confinement total. Quelques semaines suivant la simulation, un sondage fut envoyé au personnel pour avoir une vue qualitative et quantitative de la simulation pour mesurer, analyser et comparer subséquemment lors d'un prochain exercice conjoint, les résultats obtenus. Les étapes suivantes seront de partager les leçons apprises aux hôpitaux de la région ainsi qu'au service de police pour améliorer la coopération et la sécurité de nos services. La mise à jour de nos procédures, de nos aide-mémoires ainsi que la planification d'autres exercices conjoints de thème variés sera une partie prédominante des étapes futures pour la poursuite d'un apprentissage collectif pour mieux répondre en symbiose lors d'un événement.

Conclusion

Cette simulation de Code argent a démontré la valeur exceptionnelle d'un exercice conjoint entre un établissement de santé et un service de police, générant des apprentissages riches et immédiatement exploitables. Nous avons beaucoup appris, et il reste encore beaucoup à apprendre

procedures and checklists and planning other joint exercises on various topics will be a key part of the next steps in continuing our collective learning process to better respond in unison during an event.

Conclusion

This Code Silver simulation demonstrated the exceptional value of a joint exercise between a healthcare facility and a police department, generating rich and immediately actionable learning. We have learned a lot, and there is still much to learn to continue improving our level of preparedness for high-risk events. The experience with the police proved to be a real success, both operationally and collaboratively. It sparked growing interest—among facility management, staff, and police alike—in repeating this type of exercise, whether with a similar scenario or a different situation aimed at further strengthening organizational resilience.

This feedback translates the Code Silver simulation into concrete and measurable capabilities. The ERO, HRVA/HIRA, and BCP tools, as well as the procedures associated with PHIPA decision-making, provide a solid framework for structuring, consolidating, and developing organizational preparedness. Together, these elements form an essential foundation for supporting the continuous improvement of hospital resilience and ensuring a coordinated, effective, and safe response in critical situations.

Interorganizational collaboration and strategic partnerships

With a view to interorganizational collaboration and learning, several observers from other hospitals were invited to attend the simulation. Their presence served a dual purpose: to give them a concrete understanding of our approach to emergency preparedness and to obtain impartial feedback from external organizations. These observers shared rich and constructive comments, offering a different perspective on our practices and how the exercise could be replicated or adapted in their own settings.

pour continuer d'améliorer notre niveau de préparation face aux événements à haut risque. L'expérience menée avec les policiers s'est avérée un véritable succès, tant sur le plan opérationnel que collaboratif. Elle a suscité un intérêt croissant — autant au sein de la direction de l'établissement que parmi les membres du personnel et les policiers — pour renouveler ce type d'exercice, qu'il s'agisse d'un scénario similaire ou d'une mise en situation différente visant à renforcer encore davantage la résilience organisationnelle.

Ce retour d'expérience traduit la simulation de Code argent en capacités concrètes et mesurables. Les outils ERO, HRVA/HIRA, PCA ainsi que les procédures associées à la prise de décision PHIPA constituent une charpente solide pour structurer, consolider et faire évoluer la préparation organisationnelle. Ensemble, ces éléments forment un socle essentiel pour soutenir l'amélioration continue de la résilience hospitalière et assurer une réponse coordonnée, efficace et sécuritaire lors de situations critiques.

Collaboration interorganisationnelle et partenariats stratégiques

Dans une perspective de collaboration et d'apprentissage interorganisationnel, plusieurs observateurs provenant d'autres hôpitaux ont été invités à assister à la simulation. Leur présence avait un double objectif : d'une part, leur permettre de découvrir concrètement notre approche de préparation aux situations d'urgence et, d'autre part, obtenir une rétroaction impartiale provenant d'organisations externes. Ces observateurs ont partagé des commentaires riches et constructifs, offrant un regard différent sur nos pratiques et sur la manière dont l'exercice pourrait être reproduit ou adapté dans leurs propres milieux.

La simulation a également bénéficié de la participation d'un patient partenaire ainsi que d'élèves d'une école secondaire, qui

The simulation also benefited from the participation of a patient partner and high school students, who played the roles of patients and hostages. Their involvement added an extra level of realism, while incorporating diverse perspectives on the user experience during a critical event. The contribution of these non-clinical participants enhanced the educational value of the exercise and broadened the diversity of feedback received.

The participation of the police department was also a key element in the success of the activity. Very satisfied with the quality of the collaboration and the realism of the exercise, the police subsequently contacted other hospitals in the region to continue and expand the initiative begun with our institution. This spontaneous mobilization demonstrates not only the relevance of the simulation, but also the added value of our interorganizational partnership. This outreach directly contributes to promoting best practices in emergency preparedness and is fully in line with the philosophy of continuous improvement supported by Accreditation Canada and the Health Standards Organization.

Operational Risk Assessment (ORA)

Approach: Adoption of the probability × impact matrix, bowtie diagram of critical risks, and register with target controls and indicators (KPIs). Excerpt below.

Risk name	Existing controls	Priority actions
R-01 Containment of staff and customers	Lockdown button;	Automatic switchover; manual lockout, lockout procedure in place
R-02 Radio interference Police/ Admin	Single radio; Emergency line Additional equipment for first responders	2 separate networks (police/ HD); T-15 test; intelligibility audit

ont assumé les rôles de patients et d'otage. Leur implication a ajouté un niveau de réalisme supplémentaire, tout en intégrant des perspectives variées quant à l'expérience usager lors d'un événement critique. La contribution de ces participants non cliniques a renforcé la valeur pédagogique de l'exercice et a permis d'élargir la diversité des rétroactions reçues.

La participation du service de police a aussi été un élément clé de la réussite de l'activité. Très satisfaits de la qualité de la collaboration et du réalisme de l'exercice, les policiers ont par la suite communiqué avec d'autres hôpitaux de la région afin de poursuivre et d'élargir l'initiative amorcée avec notre établissement. Cette mobilisation spontanée témoigne non seulement de la pertinence de la simulation, mais aussi de la valeur ajoutée de notre partenariat interorganisationnel. Ce rayonnement contribue directement à promouvoir des pratiques exemplaires en préparation aux situations d'urgence et s'inscrit pleinement dans la philosophie d'amélioration continue soutenue par Agrément Canada et l'Organisation des normes en santé.

Évaluation des risques opérationnels (ERO)

Approche : Adoption de la matrice de probabilité × impact, diagramme en nœud papillon des risques critiques, et registre avec contrôles cibles et indicateurs (KPI). Extrait ci-dessous.

Nom du risque	Contrôles existants	Actions prioritaires
R-01 Confinement du personnel et des clients	Bouton Lockdown ;	Bascule automatique ; verrouillage manuel, procédure en place de verrouillage
R-02 Interférences radio Police/Admin	Radio unique ; Ligne d'urgence Équipement supplémentaire pour premiers répondants	2 réseaux séparés (police/HD) ; test T-15 ; audit d'intelligibilité

R-03 Message to staff	RAVE and SP/PA	Clear templates; dual channel (pop-up screen + email); logging
R-04 Police requests (PHIPA)	Privacy policy	SOP PHIPA
R-05 Concurrent Code Blue (ACR/VSA)	Clinical team; intercom	Protected routes; escorts Validated police; critical care priority
R-06 Misinformation/ social media	Media policy; Communications team	Anti-rumor procedure; bilingual publications; monitoring and rapid correction
R-07 Line saturation (on-call admin)	Emergency line; call instructions	Single number; relevance filter; live FAQ
R-08 RAVE/SP/ overhead failure	Existing redundancy	Backup plan (SMS/email/ message on screens in waiting rooms); periodic tests; IT incident SLA
R-09 Ambulance access impeded	Usual routes; vs. ambulance diversion	Marked protected lanes; checkpoints; EMS/police coordination
R-10 Congestion/ crowding at entrance (cold)	Security; public announcements	Heated staging area; non-clinical triage;
R-11 Fatigue/relief for key personnel	On-call roster; EAP, mandatory IMS training for managers	12–24-hour relief team; microbreaks; proactive EAP and short debrief
R-12 Language barriers (FR/EN)	FR/EN messages; internal translation	Bilingual templates; reading aloud; universal pictograms
R-14 Unknown crash bag (Police/ clinic)	Crash bag available	Standardized inventory; labeling; 2-minute briefing Police/ clinic upon arrival

R-03 Message au personnel	RAVE et SP/PA	Gabarits clairs ; double canal (pop-up écran + courriel) ; journalisation
R-04 Demandes des policiers (PHIPA)	Politique vie privée	SOP PHIPA
R-05 Code bleu concomitant (ACR/ VSA)	Équipe clinique ; interphone	Voies protégées ; escortes Police validées ; priorité des soins critiques
R-06 Désinformation/ médias sociaux	Politique média ; équipe des Communications	Procédure anti-rumeurs ; publications bilingues ; veille et correction rapide
R-07 Saturation des lignes (admin de garde)	Ligne d'urgence ; consignes d'appel	Numéro unique ; filtre pertinence ; FAQ en direct
R-08 Panne RAVE/ SP/overhead	Redondance existante	Plan de relève (SMS/ courriel/message sur les écrans dans les salles d'attente) ; tests périodiques ; SLA IT incident
R-09 Accès ambulances entravé	Chemins habituels ; vs détournement d'ambulance	Voies protégées balisées ; points de contrôle ; coordination EMS/ Police
R-10 Congestion/ afflux à l'entrée (froid)	Sécurité ; messages publics	Zone de repli chauffée ; triage non-clinique ;
R-11 Fatigue/relève du personnel clé	Banque de rappel ; PAE, Formation IMS obligatoire des cadres	Équipe de relève 12–24 h ; micro-pauses ; PAE proactif et debrief court
R-12 Barrières linguistiques (FR/EN)	Messages FR/ EN ; traduction interne	Gabarits bilingues ; lecture à voix haute ; pictogrammes universels
R-14 Crash bag inconnu (Police/ clinique)	Crash bag disponible	Inventaire standardisé ; étiquetage ; brief 2 min Police/clinique à l'arrivée

Implementation of professional practices

The professional practices targeted are listed in a table according to the selected standards.

Actions implemented	HSO 9002 (axis)	DRI (PP#)
Activation Silver Code	Axis 4 – Respond/Recover	PP5 – Incident Preparedness & Response
IMS/SGI activated	Axis 1 – Laying the Groundwork	PP1 – Program Management
RACI of inputs	Axis 1 – Laying the foundations	PP1 – Program Management
Police/negotiator coordination	Axis 4 – Respond/Restore	PP10 – Coordination with External Agencies
RAVE messages/general call system	Axis 3 – Prepare (plan, communicate) + Axis 4 – Respond (disseminate, coordinate)	PP9 – Crisis Communications
Media Management	Axis 4 – Respond/Restore	PP9 – Crisis Communications
Lockdown/access control	Axis 2 – Assess and reduce risks (analyze, secure) + Axis 3 – Prepare (plan, test)	PP5 – Incident Preparedness & Response
Entry/exit control	Axis 4 – Respond/Recover	PP5 – Incident Preparedness & Response
Continuity of care	Axis 3 – Prepare (plan, anticipate) + Axis 4 – Respond and recover (maintain, restore)	PP4 – Business Continuity Strategies
Code Blue with police escort	Axis 4 – Respond/Restore	PP5 – Incident Preparedness & Response + PP10 – Coordination with External Agencies
Lifting of lockdown	Axis 4 – Respond/Recover	PP5 – Incident Preparedness & Response+ PP9 – Crisis Communications
Dedicated Radios/Channels	Axis 2 – Assess and reduce risks (analyze, secure) + Axis 3 – Prepare (plan, test, communicate)	PP5 – Incident Preparedness & Response
Event log	Axis 3 – Prepare (document, plan) + Axis 4 – Respond and recover (analyze, improve)	PP8 – Exercise/Test, Assessment & Maintenance
Hot-wash/debriefing INACSL	Axis 4 – Recover	PP8 – Exercise/Test, Assessment & Maintenance
Patient information sharing (PHIPA)	Axis 1 – Laying the groundwork (governing, defining rules) + Axis 3 – Preparing (planning, communicating, securing)	PP1 – Program Management PP9 – Crisis Communications
EAP / psychosocial support	Axis 4 – Restore	PP4 – Business Continuity Strategies
Single admin on-call number	Axis 3 – Prepare	PP9 – Crisis Communications PP1 – Program Management
Skills & Training	Axis 3 – Prepare	PP7 – Awareness & Training Programs
Documentation & Continuous Improvement	Axis 1 & Axis 4	PP8 – Assessment & Maintenance

Mise en œuvre des pratiques professionnelles

Voici les pratiques professionnelles ciblées dans un tableau selon les normes choisies.

Actions mises en œuvre	HSO 9002 (axe)	DRI (PP#)
Activation Code argent	Axe 4 – Répondre/Rétablir	PP5 – Incident Preparedness & Response
IMS/SGI activé	Axe 1 – Établir les bases	PP1 – Program Management
RACI des intrants	Axe 1 – Établir les bases	PP1 – Program Management
Coordination police/négociateur	Axe 4 – Répondre/Rétablir	PP10 – Coordination with External Agencies
Messages RAVE/système d'appel général	Axe 3 – Se préparer (planifier, communiquer) + Axe 4 – Répondre (diffuser, coordonner)	PP9 – Crisis Communications
Gestion des médias	Axe 4 – Répondre/Rétablir	PP9 – Crisis Communications
Lockdown/contrôle d'accès	Axe 2 – Évaluer et réduire les risques (analyser, sécuriser) + Axe 3 – Se préparer (planifier, tester)	PP5 – Incident Preparedness & Response
Contrôle entrées/sorties	Axe 4 – Répondre/Rétablir	PP5 – Incident Preparedness & Response
Continuité des soins	Axe 3 – Se préparer (planifier, anticiper) + Axe 4 – Intervenir et se remettre (maintenir, restaurer)	PP4 – Business Continuity Strategies
Code Bleu avec escorte policière	Axe 4 – Répondre/Rétablir	PP5 – Incident Preparedness & Response + PP10 – Coordination with External Agencies
Déconfinement	Axe 4 – Répondre/Rétablir	PP5 – Incident Preparedness & Response + PP9 – Crisis Communications
Radios/canaux dédiés	Axe 2 – Évaluer et réduire les risques (analyser, sécuriser) + Axe 3 – Se préparer (planifier, tester, communiquer)	PP5 – Incident Preparedness & Response
Journal d'événements	Axe 3 – Se préparer (documenter, planifier) + Axe 4 – Intervenir et se remettre (analyser, améliorer)	PP8 – Exercise/Test, Assessment & Maintenance
Hot-wash/débriefing INACSL	Axe 4 – Rétablir	PP8 – Exercise/Test, Assessment & Maintenance
Partage info patient (PHIPA)	Axe 1 – Établir les bases (gouverner, définir les règles) + Axe 3 – Se préparer (planifier, communiquer, sécuriser)	PP1 – Program Management PP9 – Crisis Communications
PAE / soutien psychosocial	Axe 4 – Rétablir	PP4 – Business Continuity Strategies
Numéro unique admin de garde	Axe 3 – Se préparer	PP9 – Crisis Communications PP1 – Program Management
Compétences & formation	Axe 3 – Se préparer	PP7 – Awareness & Training Programs
Documentation & amélioration continue	Axe 1 & Axe 4	PP8 – Assessment & Maintenance

Liste des acronymes et abréviations

List of acronyms and abbreviations

Acronyme (FR)	Signification (FR)	Acronym (EN)	Signification (EN)
SGI	Système de gestion des incidents	IMS	Incident Management System
PCA	Plan de continuité des activités	BCP	Business Continuity Plan
ERO	Évaluation des risques opérationnels	ORA	Operational Risk Assessment
HRVA	Hazard Risk Vulnerability Analysis (méthodologie CB)	HRVA	Hazard Risk Vulnerability Analysis
HIRA	Hazard Identification and Risk Assessment (Ontario)	HIRA	Hazard Identification and Risk Assessment
HVA	Hospital Vulnerability Analysis	HVA	Hospital Vulnerability Analysis
HSI	Indice de sécurité hospitalière	HSI	Hospital Safety Index
PHIPA	Loi sur la protection des renseignements médicaux de l'Ontario	PHIPA	Personal Health Information Protection Act
RAVE	Plateforme d'alertes de masse	RAVE	Mass Notification Platform
SP	Sonorisation publique	PA	Public Address
RACI	Répartition des rôles (Responsable, etc.)	RACI	Responsible, Accountable, Consulted, Informed
KPI	Indicateurs de performance clés	KPI	Key Performance Indicators
PDCA	Planifier – Exécuter – Vérifier – Agir	PDCA	Plan – Do – Check – Act
EAC	Contrôle d'accès électronique	EAC	Electronic Access Control
CCTV	Télésurveillance en circuit fermé	CCTV	Closed-Circuit Television
ASV	Absence de signes vitaux	VSA	Vital Signs Absent
DND	Ministère de la Défense nationale (Canada)	DND	Department of National Defence
SOP	Procédure opérationnelle normalisée	SOP	Standard Operating Procedure
MSEL	Liste maîtresse des événements	MSEL	Master Scenario Events List
EMS	Services médicaux d'urgence	EMS	Emergency Medical Services
AAR	Rapport post-activité	AAR	After-Action Report
Lockdown	Confinement	Lockdown	Secure/Access Control Activation
Nœud papillon	Méthode d'analyse des barrières	Bow-Tie	Barrier Analysis Diagram

Acknowledgements

We would like to express our sincere thanks to the patient partners, stakeholders, staff members, and senior management for their commitment, availability, and essential participation in the success of this exercise. Their active involvement made it possible to recreate a realistic, safe, and highly educational environment.

We would also like to thank the communications team for their essential role in the success of this exercise: taking photos, disseminating messages before, during, and after the simulation, and providing overall support ensured effective coordination, a common understanding of objectives, and valuable documentation for post-event analysis.

Finally, we would like to thank the Ottawa Police Service for their exemplary availability and remarkable professionalism throughout the exercise. Their collaboration greatly enriched the experience and enhanced the quality of the interdisciplinary training. Ω

Remerciements

Nous tenons à exprimer nos sincères remerciements aux patients partenaires, aux acteurs, aux membres du personnel ainsi qu'à la haute direction pour leur engagement, leur disponibilité et leur participation essentielle à la réussite de cet exercice. Leur implication active a permis de recréer un environnement réaliste, sécuritaire et hautement formateur.

Nous souhaitons aussi remercier l'équipe des communications pour son rôle essentiel dans la réussite de cet exercice : la prise de photos, la diffusion des messages avant, pendant et après la simulation, ainsi que le soutien global offert ont permis d'assurer une coordination efficace, une compréhension commune des objectifs et une documentation précieuse pour l'analyse post-événement.

Finalement, nous souhaitons remercier les policiers de la Ville d'Ottawa pour leur disponibilité exemplaire et le professionnalisme remarquable qu'ils ont démontré tout au long de l'exercice. Leur collaboration a grandement enrichi l'expérience et renforcé la qualité de l'entraînement interdisciplinaire. Ω

ABOUT THE AUTHOR

Eric Corriveau *is a specialist in emergency management with more than 20 years of experience in civil security and pre hospital emergency response. A former advanced care paramedic, he has also taught paramedic sciences and emergency management at Collège La Cité and George Brown College. Co author of the HSO 9002:2020 standard, he now contributes to planning, training, and organizational resilience in the hospital sector.*

À PROPOS DE L'AUTEUR

Eric Corriveau *est spécialiste en gestion des mesures d'urgence, fort de plus de 20 ans d'expérience en sécurité civile et intervention préhospitalière. Ancien paramédic de soins avancés, il a aussi enseigné les soins ambulanciers et la gestion des urgences au Collège La Cité et au George Brown College. Co auteur de la norme HSO 9002:2020, il contribue aujourd'hui à la planification, la formation et la résilience organisationnelle en milieu hospitalier.*

An Experts' Impression

L'Impression d'un expert

Spring 2026 An Expert's Impression

IN THIS ISSUE OF TRUE NORTH RESILIENCE, WE'RE EXPLORING THE OPERATIONAL ASPECT OF CYBERSECURITY AND WHAT BUSINESS AND THOUGHT LEADERS ARE DOING TO COMBAT EVERYONE'S BIGGEST FEAR.

OPERATIONAL REALITY QUESTIONS:

- "WHAT'S THE HARDEST PART OF MAINTAINING CYBER READINESS IN YOUR INDUSTRY?"
- "WHAT SECURITY CONTROL DELIVERED THE BEST ROI THAT YOUR ORGANIZATION IMPLEMENTED RECENTLY?"
- "WHAT RESILIENCE MEASURE PROVED MORE EFFECTIVE THAN YOU EXPECTED?"

- GAT

Printemps 2026 L'avis d'un expert

DANS CE NUMÉRO DE TRUE NORTH RESILIENCE, NOUS EXPLORONS L'ASPECT OPÉRATIONNEL DE LA CYBERSÉCURITÉ ET CE QUE FONT LES CHEFS D'ENTREPRISE ET LES LEADERS D'OPINION POUR LUTTER CONTRE LA PLUS GRANDE CRAINTE DE TOUS.

QUESTIONS SUR LA RÉALITÉ OPÉRATIONNELLE :

- « QUELLE EST LA PARTIE LA PLUS DIFFICILE DU MAINTIEN DE LA CYBERPRÉPARATION DANS VOTRE SECTEUR ? »
- « QUELLE MESURE DE SÉCURITÉ MISE EN ŒUVRE RÉCEMMENT PAR VOTRE ORGANISATION A GÉNÉRÉ LE MEILLEUR RETOUR SUR INVESTISSEMENT ? »
- « QUELLE MESURE DE RÉSILIENCE S'EST AVÉRÉE PLUS EFFICACE QUE PRÉVU ? »

- GAT

An Expert's Impression

Robert Munden:

"What's the hardest part of maintaining cyber readiness in your industry?"

The combined pace of change of underlying technologies deployed in and for customers, multiplied by the similar rate of change in security tools and tactics. There are few truly long-term solutions except at the highest level of generality. This creates a continuing burden relating to implementing and retiring tools and technology, managing the change process for that with customers, an0d training for internal staff.

Ann Wyganowski:

"What's the hardest part of maintaining cyber readiness in your industry?"

AI and the ability of governments to regulate or control the use of AI is setting a whole new stage for cyber risk. Generally speaking, any democratic government is notoriously slow in its ability to pass legislation or agree upon an approach to regulation in industry sectors. Those who will profit from unchecked powers to advance AI will seek to influence government officials in various ways to advance their intentions, which are largely undefined or not well understood at this time. There are pockets of understanding about the massive toll on existing electrical grids from large data centres used for AI, but not a great understanding of how state sponsored bad actors in the cyber world are using the opportunity to advance their abilities. AI can further their abilities to exploit zero-day weaknesses

L'impression d'un expert

Robert Munden :

« Quel est l›aspect le plus difficile du maintien de la cyberpréparation dans votre secteur ? »

Le rythme combiné des changements des technologies sous-jacentes déployées chez et pour les clients, multiplié par le rythme similaire des changements dans les outils et les tactiques de sécurité. Il existe peu de solutions véritablement durables, sauf au plus haut niveau de généralité. Cela crée une charge permanente liée à la mise en œuvre et au retrait des outils et des technologies, à la gestion du processus de changement auprès des clients et à la formation du personnel interne.

Ann Wyganowski :

« Quel est l›aspect le plus difficile du maintien de la cyberpréparation dans votre secteur ? »

L'IA et la capacité des gouvernements à réglementer ou contrôler son utilisation ouvrent une toute nouvelle perspective en matière de cyberrisques. D'une manière générale, les gouvernements démocratiques sont connus pour leur lenteur à adopter des lois ou à s'accorder sur une approche réglementaire dans les différents secteurs industriels. Ceux qui tireront profit d'un pouvoir illimité pour faire progresser l'IA chercheront à influencer les responsables gouvernementaux de diverses manières afin de faire avancer leurs intentions, qui sont pour l'instant largement indéfinies ou mal comprises. Il existe une certaine compréhension des conséquences considérables des grands centres de données utilisés pour l'IA sur les réseaux électriques existants, mais on ne comprend pas très bien comment les acteurs malveillants soutenus

discovered in ways we can›t easily imagine. Cyber Resilience is the new way forward. Every continuity and resilience professional should be thinking about becoming a (Certified Cyber Resilience Professional) CCRP as their next level of excellence in their career. It›s a step up from Business Continuity.

"What security control delivered the best ROI that your organization implemented recently?"

The human firewall is the best ROI in any organization, but the investment in a proper IT Disaster Recovery strategy and plan is needed to ensure a timely recovery from a cyber incident. The greater the awareness and training in the techniques being implemented to breach any organizations security, the better off the organization will be. If the organization is willing to spend the time in effectively developing the awareness and training in cyber risk, showing leadership support, as well as making the employees' time investment commensurate with the risk, then employees will take the knowledge transfer seriously. The resulting diligence in protecting the organization can reap many rewards. An employer should not stop at the perimeter of the organization though; by educating employees about the kinds of cyber risks and scams that can affect them personally, as well as the potential consequences has a far-reaching effect. Staff who feel that their employer is looking out for them will build loyalty to their organization and feel they are part of a team. Isolation and siloing of 'team members' created during the pandemic needs to be addressed as part of rebuilding that 'corporate culture' and social framework in any organization. As the hybrid work

par des États dans le monde cybernétique exploitent cette opportunité pour développer leurs capacités. L'IA peut renforcer leur capacité à exploiter les faiblesses zero-day découvertes d'une manière que nous ne pouvons pas facilement imaginer. La cyber-résilience est la nouvelle voie à suivre. Tous les professionnels de la continuité et de la résilience devraient envisager de devenir CCRP (Certified Cyber Resilience Professional) afin d'atteindre un niveau d'excellence supérieur dans leur carrière. Il s'agit d'une étape supplémentaire par rapport à la continuité des activités.

« Quelle mesure de sécurité mise en œuvre récemment par votre organisation a généré le meilleur retour sur investissement ? »

Le pare-feu humain est le meilleur retour sur investissement dans toute organisation, mais il est nécessaire d'investir dans une stratégie et un plan de reprise après sinistre informatique appropriés pour garantir une reprise rapide après un cyberincident. Plus la sensibilisation et la formation aux techniques mises en œuvre pour compromettre la sécurité d'une organisation sont importantes, mieux l'organisation se portera. Si l'organisation est prête à consacrer du temps à développer efficacement la sensibilisation et la formation aux risques cybernétiques, à montrer le soutien de la direction et à faire en sorte que l'investissement en temps des employés soit proportionnel au risque, alors les employés prendront au sérieux le transfert de connaissances. La diligence qui en résulte pour protéger l'organisation peut être très profitable. Un employeur ne doit toutefois pas s'arrêter au périmètre de l'organisation ; en sensibilisant les employés aux types de cyberrisques et d'escroqueries qui peuvent les toucher personnellement, ainsi qu'aux conséquences potentielles, il aura un effet considérable. Les employés qui sentent que leur employeur veille sur eux développeront leur loyauté envers leur organisation et auront le sentiment de faire partie d'une équipe. L'isolement et le cloisonnement des « membres de l'équipe » créés pendant la pandémie doivent être traités dans le cadre de

environment becomes more firmly entrenched employees are pushing back on full return to the physical office full time. Organizations need to balance the risks associated with the hybrid work environment while building the human firewall stronger, and this is an opportunity to do so in a positive way. IT Disaster Recovery (DR) plans need to be better understood in relation to the cyber risks and updated accordingly. Our 2-day Workshop in IT DR Planning has recently been updated to address the current risk environment. Many IT DR plans are traditional and haven't fully considered the impacts of a cyber attack on their organization. Strategies and properly documented plans to ensure backups are clean and there is a safe environment to recover when the inevitable happens are one of the best investments any organization can make.

"What resilience measure proved more effective than you expected?"

Professional Practice 7 - Awareness and Training is at the top of my list. We witnessed one client stop a major breach dead in its tracks due to the level of awareness at an executive level and ability to recognize extremely sophisticated whaling attacks. The use of social media has expanded by leaps and bounds. The Signal Chat scandal is just one example of many where overzealous senior officials exposed sensitive data on what they thought was a secured form of social media. As the cyber criminals exploit the personal information that individuals post in social media, it becomes increasingly easy for them to create these forms of phishing attacks and combined with AI to create even more convincing fake personas. Unless you are a Cyber Resilience and Security

la reconstruction de la « culture d'entreprise » et du cadre social de toute organisation. À mesure que l'environnement de travail hybride s'installe durablement, les employés rechignent à retourner à plein temps au bureau physique. Les organisations doivent trouver un équilibre entre les risques associés à l'environnement de travail hybride et le renforcement du pare-feu humain, et c'est l'occasion de le faire de manière positive. Les plans de reprise après sinistre (DR) informatique doivent être mieux compris en relation avec les cyber-risques et mis à jour en conséquence. Notre atelier de deux jours sur la planification de la reprise après sinistre informatique a récemment été mis à jour pour tenir compte de l'environnement de risque actuel. De nombreux plans de reprise après sinistre informatique sont traditionnels et ne tiennent pas pleinement compte des répercussions d'une cyberattaque par e sur leur organisation. Les stratégies et les plans correctement documentés visant à garantir la propreté des sauvegardes et l'existence d'un environnement sûr pour la reprise lorsque l'inévitable se produit constituent l'un des meilleurs investissements que toute organisation puisse faire.

« Quelle mesure de résilience s›est avérée plus efficace que prévu ? »

La pratique professionnelle n° 7, « Sensibilisation et formation », figure en tête de ma liste. Nous avons vu un client mettre fin à une violation majeure grâce au niveau de sensibilisation de ses dirigeants et à leur capacité à reconnaître des attaques de type « whaling » extrêmement sophistiquées. L'utilisation des réseaux sociaux s'est développée à pas de géant. Le scandale Signal Chat n'est qu'un exemple parmi tant d'autres où des hauts fonctionnaires trop zélés ont exposé des données sensibles sur ce qu'ils pensaient être un réseau social sécurisé. À mesure que les cybercriminels exploitent les informations personnelles que les individus publient sur les réseaux sociaux, il leur devient de plus en plus facile de créer ces formes d'attaques de phishing et, combinées à l'IA, de créer des faux profils encore plus convaincants.

firm, that's not what your people are there to do everyday - they are there to perform the critical business functions that the organization is there to deliver. The best way to protect the organization and its delivery of the products and services it exists to provide is to educate and protect its people. It's an investment, but a very necessary and worthwhile one to mitigate the risks. Again, the CRLE 2000 and CRLE 501 courses are an excellent way to ensure you understand what is needed in our current cyber risk environment.

Keith Barrett:

"What's the hardest part of maintaining cyber readiness in your industry?"

Working in the municipal government environment, one of the biggest challenges to cyber readiness is the sheer volume of interactions we manage every day. It is critical that staff remain current with cybersecurity awareness training so they can recognize potential phishing attempts and distinguish legitimate requests from those intended to cause harm. To support this, staff complete annual training, and we run simulated phishing exercises throughout the year to reinforce awareness and keep knowledge up to date.

"What security control delivered the best ROI that your organization implemented recently?"

We recently implemented an Extended Detection and Response (XDR) solution, which enables us to collect and correlate data from multiple sources. While individual data sets provide limited insight on their own, connecting them delivers significantly improved visibility into potential threats targeting our assets. This capability also supports 24/7/365

À moins que vous ne soyez une entreprise spécialisée dans la cyber-résilience et la cybersécurité, ce n'est pas le travail quotidien de vos employés : ils sont là pour remplir les fonctions commerciales essentielles que l'organisation est censée fournir. La meilleure façon de protéger l'organisation et la fourniture des produits et services pour lesquels elle existe est d'éduquer et de protéger ses employés. Il s'agit d'un investissement, mais il est très nécessaire et utile pour atténuer les risques. Encore une fois, les cours CRLE 2000 et CRLE 501 sont un excellent moyen de vous assurer que vous comprenez ce qui est nécessaire dans notre environnement actuel de cyber-risques.

Keith Barrett :

« Quelle est la partie la plus difficile du maintien de la cyberpréparation dans votre secteur ? »

Dans le cadre du travail au sein d'une administration municipale, l'un des plus grands défis en matière de cyberpréparation est le volume considérable d'interactions que nous gérons chaque jour. Il est essentiel que le personnel reste à jour dans sa formation à la sensibilisation à la cybersécurité afin de pouvoir reconnaître les tentatives potentielles d'hameçonnage et distinguer les demandes légitimes de celles qui visent à causer du tort. Pour soutenir cet effort, le personnel suit une formation annuelle et nous organisons des exercices de simulation d'hameçonnage tout au long de l'année afin de renforcer la sensibilisation et de maintenir les connaissances à jour.

« Quelle mesure de sécurité mise en œuvre récemment par votre organisation a généré le meilleur retour sur investissement ? »

Nous avons récemment mis en place une solution de détection et de réponse étendues (XDR), qui nous permet de collecter et de corréler des données provenant de plusieurs sources. Si les ensembles de données individuels fournissent à eux seuls des informations limitées, leur mise en relation offre une visibilité nettement améliorée sur les menaces potentielles qui pèsent sur nos actifs. Cette fonctionnalité permet également une détection

detection and response, ensuring that incidents occurring outside of regular business hours can be identified and addressed immediately.

"What resilience measure proved more effective than you expected?"

The use of MultiFactor Authentication (MFA) has significantly reduced the number of compromised accounts. While we continue to require strong passwords that are changed regularly, MFA provides an additional layer of protection by ensuring that even if a password is compromised, external threats are unable to access the account. Depending on the account type, different MFA methods are used, ranging from authenticator applications to hardware security keys.

Kevin Powers:

"What's the hardest part of maintaining cyber readiness in your industry?"

I'd say part of it is the nature of client service. Rather than a singular point of contact, all of our Lawyers are publicly listed and easy to track down for targeted attacks.

"What security control delivered the best ROI that your organization implemented recently?"

CrowdStrike on all endpoints for real time monitoring and blocking has allowed us to react much quicker, proactively even.

"What resilience measure proved more effective than you expected?"

Simulated phishing attacks, training, and remedial training. We have seen lower instances of click-through on malicious links. It has raised calls to our help desk, but id rather we field a call asking over replacing a PC.

et une réponse 24 heures sur 24, 7 jours sur 7 et 365 jours par an, garantissant ainsi que les incidents survenant en dehors des heures de bureau peuvent être identifiés et traités immédiatement.

« Quelle mesure de résilience s›est avérée plus efficace que prévu ? »

L'utilisation de l'authentification multifactorielle (MFA) a considérablement réduit le nombre de comptes compromis. Bien que nous continuions à exiger des mots de passe forts qui sont changés régulièrement, la MFA offre une couche de protection supplémentaire en garantissant que même si un mot de passe est compromis, les menaces externes ne peuvent pas accéder au compte. Selon le type de compte, différentes méthodes MFA sont utilisées, allant des applications d'authentification aux clés de sécurité matérielles.

Kevin Powers :

« Quelle est la partie la plus difficile dans le maintien de la cyberpréparation dans votre secteur ? »

Je dirais que cela tient en partie à la nature même du service à la clientèle. Plutôt que d'avoir un point de contact unique, tous nos avocats sont répertoriés publiquement et faciles à localiser pour des attaques ciblées.

« Quelle mesure de sécurité mise en œuvre récemment par votre organisation a généré le meilleur retour sur investissement ? »

CrowdStrike sur tous les terminaux pour la surveillance et le blocage en temps réel nous a permis de réagir beaucoup plus rapidement, voire de manière proactive.

« Quelle mesure de résilience s›est avérée plus efficace que prévu ? »

Les simulations d'attaques de phishing, les formations et les formations de rattrapage. Nous avons constaté une diminution du nombre de clics sur des liens malveillants. Cela a entraîné une augmentation des appels à notre service d'assistance, mais je préfère recevoir un appel pour demander le remplacement d'un PC.

ABOUT THE EXPERTS

Robert Munden *serves as Chief Legal & Compliance Officer for ESO, a leading provider of data and software solutions to EMS, fire departments and hospitals. Prior to his role at ESO, he served in legal roles in a variety of data-intensive businesses, including Harte Hanks, Safeguard Scientifics, TNS (now part of WPP) and Naviant. [optional: He received his law degree from the University of Texas at Austin, and his undergraduate degree from the U.S. Military Academy at West Point.]*

Ann Wyganowski *MBCP, CCRP is a Certified Business Continuity Professional with years of Program and Project Management experience over a wide range of industries and business functions. She has successfully implemented large scale, holistic business continuity programs and managed BCP activation during major business disruptions resulting in no lost revenues and thank you's from my clients' customers. Ann is Interested in new challenges in developing program plans or implementing BCP or disaster recovery plans. Her specialties include managing teams of people to develop, enhance, redesign and implement new business processes, business continuity plans, and business applications with particular emphasis on program and project management, new procedures, business analysis, development, roll outs, conversions, disaster recovery planning, training, documentation, retiring old procedures and applications.*

À PROPOS DES EXPERTS

Robert Munden *occupe le poste de directeur juridique et de la conformité chez ESO, l'un des principaux fournisseurs de solutions logicielles et de données destinées aux services médicaux d'urgence, aux pompiers et aux hôpitaux. Avant d'occuper ce poste chez ESO, il a occupé diverses fonctions juridiques dans plusieurs entreprises traitant d'importants volumes de données, notamment Harte Hanks, Safeguard Scientifics, TNS (qui fait désormais partie de WPP) et Naviant. [Facultatif : il est titulaire d'un diplôme en droit de l'université du Texas à Austin et d'un diplôme de premier cycle de l'Académie militaire américaine de West Point.]*

Ann Wyganowski, *MBCP, CCRP est une professionnelle certifiée de la continuité des activités avec des années d'expérience en gestion de programmes et de projets dans un large éventail d'industries et de fonctions commerciales. Elle a mis en œuvre avec succès des programmes de continuité des activités holistiques à grande échelle et a géré l'activation de la PCA lors d'interruptions majeures des activités, ce qui n'a entraîné aucune perte de revenus, et merci aux clients de mes clients. Ann s'intéresse aux nouveaux défis liés à l'élaboration de plans de programme ou à la mise en œuvre de plans de PCA ou de reprise après sinistre. Ses spécialités comprennent la gestion d'équipes de personnes pour développer, améliorer, repenser et mettre en œuvre de nouveaux processus opérationnels, des plans de continuité des activités et des applications opérationnelles, en mettant particulièrement l'accent sur la gestion de programmes et de projets, les nouvelles procédures, l'analyse opérationnelle, le développement, les déploiements, les conversions, la planification de la reprise après sinistre, la formation, la documentation, le retrait des anciennes procédures et applications.*

ABOUT THE EXPERTS

***Keith Barrett**, Director, Corporate Information Services, City of St. John's oversees strategic information systems planning, cyber and information risk management, and the reliability of complex business applications and networks that support critical municipal services. Before joining the City, Keith held senior leadership roles with the Government of Newfoundland and Labrador's Office of the Chief Information Officer, including Director of Solution Delivery and Director of Application Services. Keith has over 20 years of experience leading multi disciplinary technical teams, delivering secure, high value services, and translating complex technology issues for staff and the public.*

***Kevin Powers** is a seasoned IT leader with over 20 years of experience supporting a prominent Bay Street law firm in Toronto, an avid shade-tree mechanic, and an advocate for those with Down syndrome.*

Ω

À PROPOS DES EXPERTS

***Keith Barrett**, directeur, Services d'information d'entreprise, ville de St. John's supervise la planification stratégique des systèmes d'information, la gestion des risques liés à la cybersécurité et à l'information, ainsi que la fiabilité des applications et des réseaux commerciaux complexes qui soutiennent les services municipaux essentiels. Avant de rejoindre la ville, Keith a occupé des postes de direction au sein du bureau du directeur des systèmes d'information du gouvernement de Terre-Neuve-et-Labrador, notamment ceux de directeur de la fourniture de solutions et de directeur des services d'application. Keith a plus de 20 ans d'expérience dans la direction d'équipes techniques multidisciplinaires, la fourniture de services sécurisés et à forte valeur ajoutée, et la traduction de questions technologiques complexes pour le personnel et le public.*

***Kevin Powers** est un leader chevronné en TI avec plus de 20 ans d'expérience dans le soutien d'un important cabinet d'avocats de Bay Street à Toronto, un fervent mécanicien d'arbres d'ombrage et un défenseur des personnes atteintes du syndrome de Down.*

Ω

Adaptive Business Continuity Management for Extreme Weather Risks

Gestion adaptative de la continuité des activités face aux risques liés aux conditions météorologiques extrêmes

By/Par **Vito Mangialardi**

Abstract

This article is for risk, business continuity, and resilience practitioners who create and protect value in an organization by managing risks, making decisions in support of mitigation strategies, and setting and achieving objectives with operational (or organizational) resilience in mind.

Climate change is top of mind for decision-makers around the world. It is no easy task to work to mitigate its impacts while adapting to the now-visible consequences. It will require more resources in the years to come.

We know the climate is changing, causing extreme weather as we have never seen before. There is increasing awareness of the need to adapt both to climate change and the impact of the severe weather events – floods, hurricanes, forest fires, etc. – that are becoming increasingly frequent.

Résumé

Cet article s'adresse aux professionnels du risque, de la continuité des activités et de la résilience qui créent et protègent la valeur d'une organisation en gérant les risques, en prenant des décisions à l'appui des stratégies d'atténuation et en fixant et atteignant des objectifs dans une optique de résilience opérationnelle (ou organisationnelle).

Le changement climatique est au cœur des préoccupations des décideurs du monde entier. Il n'est pas facile de s'efforcer d'atténuer ses effets tout en s'adaptant aux conséquences désormais visibles. Cela nécessitera davantage de ressources dans les années à venir.

Nous savons que le climat change, provoquant des conditions météorologiques extrêmes comme nous n'en avons jamais connues auparavant.

In addition to thinking globally about climate change's impact, organizations must look locally at the impact it can have on their operations.

The United Nations Educational, Scientific and Cultural Organization Education UNESCO said that:

'Climate Change education and awareness are essential to the global response to climate change. It helps people understand and address the impact of global warming, increases "climate literacy" among young people, encourages changes in their attitudes and behavior and helps them adapt to climate change-related trends. Education and awareness-raising enable informed decision-making, play an essential role in increasing adaptation and mitigation capacities of communities, and empower women and men to adopt sustainable lifestyles.'

This paper joins the ongoing discussion about climate change, extreme weather, and its impacts. It explores thoughts and ideas on how business continuity planning can lead your organization to operational resiliency.

This paper endeavors to demystify climate change and adaptation as well as Enterprise Risk Management (ERM) and Business Continuity Management (BCM). By considering these together, management leaders can work towards establishing a climate-resilient organization. Resilience has many features, phases, and domains, as shown in chart 1 below. We have two fields of interest – Organizational and Engineering & Infrastructure.

On prend de plus en plus conscience de la nécessité de s'adapter à la fois au changement climatique et à l'impact des phénomènes météorologiques violents – inondations, ouragans, incendies de forêt, etc. – qui deviennent de plus en plus fréquents. En plus de réfléchir à l'échelle mondiale à l'impact du changement climatique, les organisations doivent examiner localement l'impact qu'il peut avoir sur leurs activités.

L'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO) a déclaré[AL1] :

« L'éducation et la sensibilisation au changement climatique sont essentielles à la réponse mondiale au changement climatique. Elles aident les gens à comprendre et à faire face à l'impact du réchauffement climatique, améliorent la « culture climatique » des jeunes, encouragent les changements dans leurs attitudes et leurs comportements et les aident à s'adapter aux tendances liées au changement climatique. L'éducation et la sensibilisation permettent une prise de décision éclairée, jouent un rôle essentiel dans le renforcement des capacités d'adaptation et d'atténuation des communautés, et donnent aux femmes et aux hommes les moyens d'adopter des modes de vie durables. »

Cet article s'inscrit dans le débat actuel sur le changement climatique, les phénomènes météorologiques extrêmes et leurs impacts. Il explore des réflexions et des idées sur la manière dont la planification de la continuité des activités peut conduire votre organisation à la résilience opérationnelle.

Ce document s'efforce de démystifier le changement climatique et l'adaptation, ainsi que la gestion des risques d'entreprise (ERM) et la gestion de la continuité des activités (BCM). En considérant ces éléments ensemble, les dirigeants peuvent œuvrer à la mise en place d'une organisation résiliente au changement climatique. La résilience comporte de nombreuses caractéristiques, phases et domaines, comme le montre le tableau 1 ci-dessous. Nous avons deux domaines d'intérêt : l'organisation et l'ingénierie et les infrastructures.

Chart 1: The National Academy of Science's definition of resilience identifies several temporal phases.

NAS Phase of Resilience	Resilience Feature	Description by Application Domain			
		Socio-Ecological	Psychological	Organizational	Engineering & Infrastructure
Plan	Critical Function	A system function identified by stakeholders as an essential dimension by which to assess system performance			
		Ecosystem Services provided to society	Human psychological well-being	Goods and services provided to society	Services provided by physical and technical engineered systems
Absorb	Threshold	Intrinsic tolerance to stress or changes in conditions where exceeding a threshold perpetuates a regime shift			
		Used to identify natural breaks in scale	Based on a sense of community and personal attributes	Linked to adaptive organizational capacity and brittleness when close to the threshold	Based on the sensitivity of system functioning to changes in input variables
Recover	Time	Duration of degraded system performance			
		Emphasis on dynamics over time	Emphasis on time of disruption (i.e., developmental stage: childhood vs. adulthood)	Emphasis on time until recovery	Focus on time until recovery
Adapt	Memory/Adaptive Management	Change in management approach or other responses in anticipation of or enabled by learning from previous disruptions, events, or experiences			
		Ecological memory guides how ecosystems reorganize after a disruption, which is maintained if the system has high modularity	Human and social memory can enhance (through learning) or diminish (e.g., post-traumatic stress) psychological resilience	Corporate memory of challenges posed to the organization and management that enable modification and building of responsiveness to events	Re-designing of engineering systems designs based on past and potent

With operational resilience to climate change as the goal, the following policy standards should be applied:

- Adapting business continuity practices to evaluate and mitigate (build resilience) to weather variability (changing climate) with the objective of long-term sustainability.
- Asking the organization cause a negative impact on the environment and if the effects of climate change and extreme weather event will impact the business.
- Including the supply chain partners and vendors in the risk assessments and delivery expectations; and I am using an extreme weather-related scenario when exercising (or testing) your Business Continuity Plan (BCP), following an exercise plan template, documenting the outputs, and using them to revise the plan.

This paper shares general thoughts and ideas for all sizes of business organizations to consider when connecting risk management, business continuity planning, and climate change adaptation as they make plans to keep their operations running when future extreme weather incidents impact their business.

Graphique 1 : La définition de la résilience donnée par l'Académie nationale des sciences identifie plusieurs phases temporelles.

Phase NAS de résilience	Caractéristique de résilience	Description par domaine d'application			
		Socio-écologique	Psychologique	Organisationnel	Ingénierie et infrastructure
Plan	Fonction critique	Fonction du système identifiée par les parties prenantes comme une dimension essentielle pour évaluer la performance du système			
		Services écosystémiques fournis à la société	Bien-être psychologique humain	Biens et services fournis à la société	Services fournis par les systèmes physiques et techniques
Absorber	Seuil	Tolérance intrinsèque au stress ou aux changements de conditions où le dépassement d'un seuil entraîne un changement de régime			
		Utilisé pour identifier les ruptures naturelles d'échelle	Basé sur le sens de la communauté et les attributs personnels	Lié à la capacité d'adaptation organisationnelle et à la fragilité lorsque le seuil est proche	Basé sur la sensibilité du fonctionnement du système aux changements des variables d'entrée
Récupération	Temps	Durée de la dégradation des performances du système			
		Accent mis sur la dynamique au fil du temps	Accent mis sur le moment de la perturbation (c'est-à-dire le stade de développement : enfance vs âge adulte)	Accent mis sur le temps nécessaire à la récupération	Accent mis sur le temps nécessaire à la guérison
Adapt	Mémoire/gestion adaptative	Changement d'approche de gestion ou autres réponses anticipées ou rendues possibles par les enseignements tirés des perturbations, événements ou expériences antérieurs			
		La mémoire écologique guide la manière dont les écosystèmes se réorganisent après une perturbation, qui est maintenue si le système présente une modularité élevée	La mémoire humaine et sociale peut renforcer (par l'apprentissage) ou affaiblir (par exemple, le stress post-traumatique) la résilience psychologique	Mémoire collective des défis posés à l'organisation et à la gestion qui permettent de modifier et de renforcer la réactivité face aux événements	Refonte de la conception des systèmes d'ingénierie sur la base du passé et du potentiel

Dans le but d'assurer la résilience opérationnelle face au changement climatique, les normes politiques suivantes doivent être appliquées :

- Adapter les pratiques de continuité des activités afin d'évaluer et d'atténuer (renforcer la résilience) les variations climatiques (changement climatique) dans une optique de durabilité à long terme.
- Demander à l'organisation si elle a un impact négatif sur l'environnement et si les effets du changement climatique et des phénomènes météorologiques extrêmes auront une incidence sur ses activités.
- Inclure les partenaires de la chaîne d'approvisionnement et les fournisseurs dans les évaluations des risques et les attentes en matière de livraison ; et j'utilise un scénario lié à des conditions météorologiques extrêmes lorsque j'exerce (ou teste) votre plan de continuité des activités (PCA), en suivant un modèle de plan d'exercice, en documentant les résultats et en les utilisant pour réviser le plan.

Ce document présente des réflexions et des idées générales que les entreprises de toutes tailles peuvent prendre en compte lorsqu'elles établissent un lien entre la gestion des risques, la planification de la continuité des activités et l'adaptation au changement climatique, afin de prévoir des plans pour maintenir leurs opérations lorsque des phénomènes météorologiques extrêmes auront un impact sur leurs activités.

Preface:

This article was written during the COVID-19 pandemic, so the learnings from this time can be applied to all BCM scenarios, including severe weather. One of these lessons is that threats to our businesses do not always happen in isolation. More often than not, we have cascading or multiple events co-occurring and must plan to deal with several challenges at once. For example, as the climate changes, we have seen hotter summers and more intense forest fires in recent years – a pattern independent of the pandemic. As a result, firefighters working to save forests are dealing with two global issues simultaneously. So, along with the usual health and safety considerations, they now need to overlay efforts of following public health measures to protect against COVID-19.

Climate Change Refresher

As a public and policy issue, climate change boils down to four overarching topics: [1]

1. The climate is changing.
2. People are causing the environment to change.
3. The societal consequences of climate change are highly uncertain but include the potential for severe impacts; and
4. There are numerous policy options for climate change risk management, most of which are well characterized (i.e., have known strengths and weaknesses).

Climate change risk management approaches generally fall into four broad categories:

1. **Mitigation**—efforts to reduce greenhouse gas emissions.
2. **Adaptation**—increasing society's capacity to cope with changes in climate.
3. **Geoengineering or climate engineering**—the additional, deliberate manipulation of the earth system that is intended to counteract at least some of the impacts of greenhouse gas emissions; and

[1] American Meteorological Society Policy Program Study October 2014 (Key Findings and Recommendations)

Préface :

Cet article a été rédigé pendant la pandémie de COVID-19, mais les enseignements tirés de cette période peuvent s'appliquer à tous les scénarios de gestion de la continuité des activités (BCM), y compris les conditions météorologiques extrêmes. L'un de ces enseignements est que les menaces qui pèsent sur nos entreprises ne se produisent pas toujours de manière isolée. Le plus souvent, nous sommes confrontés à une succession d'événements ou à plusieurs événements simultanés et devons nous préparer à relever plusieurs défis à la fois. Par exemple, avec le changement climatique, nous avons connu des étés plus chauds et des incendies de forêt plus intenses ces dernières années, une tendance indépendante de la pandémie. En conséquence, les pompiers qui s'efforcent de sauver les forêts sont confrontés simultanément à deux problèmes mondiaux. Ainsi, outre les considérations habituelles en matière de santé et de sécurité, ils doivent désormais redoubler d'efforts pour respecter les mesures de santé publique visant à se protéger contre la COVID-19.

Rappel sur le changement climatique

En tant que question publique et politique, le changement climatique se résume à quatre thèmes généraux :[1]

1. Le climat change.
2. Les humains sont à l'origine des changements environnementaux.
3. Les conséquences sociétales du changement climatique sont très incertaines, mais peuvent avoir des répercussions graves.
4. Il existe de nombreuses options politiques pour gérer les risques liés au changement climatique, dont la plupart sont bien caractérisées (c'est-à-dire que leurs forces et leurs faiblesses sont connues).

Les approches de gestion des risques liés au changement climatique se répartissent généralement en quatre grandes catégories :

[1] Étude sur le programme politique de l'American Meteorological Society, octobre 2014 (principales conclusions et recommandations)

4. **Knowledgebase expansion**—efforts to learn and understand more about the climate system can help support proactive risk management.

From all definitions for climate change that exist, A simplistic standard explanation by Wikipedia is that Climate Change can be understood as proactively planning (both short term and long term) for the adverse effects of (typically) extreme weather-caused climate change. This includes implementing appropriate actions (known as risk controls[2]) to address the resulting negative eliminate or taking advantage of opportunities that may present themselves.

During the January 2018 World Economic Forum, it was noted that "Climate change would shape how we do business for decades. The business has a vital role in curbing its effects by limiting carbon emissions, but success isn't just about action from individual companies. To create change on a level large enough to halt climate change, businesses – and whole sectors and value chains – will need to consolidate efforts.[3] "

Wikipedia summed up that best by saying, "The main effect is an increasing global average temperature. The average surface temperature could increase by 3 to 10 degrees Fahrenheit (approximately 1.67 to 5.56 degrees Celsius) by the end of the century if carbon emissions aren't reduced .[4]"

Efforts to reduce carbon dioxide emissions, and the resulting greenhouse effect, have

[2] Investopedia: Risk control is the set of methods by which firms evaluate potential losses and take action to reduce or eliminate such threats. It is a technique that utilizes findings from risk assessments. Risk control methods include avoidance, loss prevention, loss reduction, separation, duplication, and diversification) to address the resulting negative eliminate or taking advantage of opportunities that may present themselves.

[3] January 2018 - World Economic Forum: Two Degrees of Transformation Businesses are coming together to lead on climate change. Will you join them?

[4] From Wikipedia - https://en.wikipedia.org/wiki/Climate_change_adaptation

1. **Atténuation :** efforts visant à réduire les émissions de gaz à effet de serre.
2. **Adaptation :** augmentation de la capacité de la société à faire face aux changements climatiques.
3. **Géo-ingénierie ou ingénierie climatique :** manipulation supplémentaire et délibérée du système terrestre visant à contrebalancer au moins certains des impacts des émissions de gaz à effet de serre.
4. **Élargissement de la base de connaissances :** les efforts visant à mieux connaître et comprendre le système climatique peuvent contribuer à une gestion proactive des risques.

Parmi toutes les définitions existantes du changement climatique, Wikipédia en donne une explication standard simplifiée : le changement climatique peut être compris comme une planification proactive (à court et à long terme) des effets néfastes du changement climatique (généralement) causé par des conditions météorologiques extrêmes. Cela comprend la mise en œuvre de mesures appropriées (appelées contrôles des risques[2]) pour éliminer les effets négatifs qui en résultent ou tirer parti des opportunités qui peuvent se présenter.

Lors du Forum économique mondial de janvier 2018, il a été noté que « le changement climatique façonnerait notre façon de faire des affaires pendant des décennies. Les entreprises ont un rôle essentiel à jouer dans la lutte contre ses effets en limitant les émissions de carbone, mais le succès ne dépend pas uniquement des actions individuelles des entreprises. Pour créer un changement suffisamment important pour enrayer le changement climatique, les

2 Investopedia : Le contrôle des risques est l'ensemble des méthodes utilisées par les entreprises pour évaluer les pertes potentielles et prendre des mesures afin de réduire ou d'éliminer ces menaces. Il s'agit d'une technique qui utilise les résultats des évaluations des risques. Les méthodes de contrôle des risques comprennent l'évitement, la prévention des pertes, la réduction des pertes, la séparation, la duplication et la diversification afin d'éliminer les conséquences négatives ou de tirer parti des opportunités qui peuvent se présenter.

focused on two items, reducing carbon pollution and preparing for the consequences of global warming. In business continuity planning, we must look at the impacts of one particular outcome – a growing number of extreme weather events. This year (2021) alone, we have had…

While planning for organizational resiliency, we must address the ever-increasing pattern of unexpected, unseasonal, unusual, and extreme weather events. These include extreme temperatures, drought, heavy rainfall, lightning storms, freezing rain, snow, changing freeze-thaw cycles, frost, hail, high winds, and tornadoes. This can lead to other impacts, such as rising sea levels and intense droughts, threatening crops, wildlife, and freshwater supplies. Some examples from my public commuter rail transit experience of things that have become common now are our tracks and bus routes…

Organizations are awakening to the dangers posed by climate change and extreme weather. Climate and environmental assessments continue to rank it as a dominating risk. According to CEOs from around the world surveyed for a World Economic Forum report presented

entreprises, ainsi que l'ensemble des secteurs et des chaînes de valeur, devront consolider leurs efforts. [3]»

Wikipédia résume bien la situation en affirmant que « le principal effet est une augmentation de la température moyenne mondiale. La température moyenne à la surface pourrait augmenter de 3 à 10 degrés Fahrenheit (environ 1,67 à 5,56 degrés Celsius) d'ici la fin du siècle si les émissions de carbone ne sont pas réduites [4]».

Les efforts visant à réduire les émissions de dioxyde de carbone et l'effet de serre qui en résulte se sont concentrés sur deux points : la réduction de la pollution par le carbone et la préparation aux conséquences du réchauffement climatique. Dans le cadre de la planification de la continuité des activités, nous devons examiner les impacts d'un résultat particulier : le nombre croissant de phénomènes météorologiques extrêmes. Rien que cette année (2021), nous avons eu...

Lors de la planification de la résilience organisationnelle, nous devons tenir compte de la fréquence croissante des phénomènes météorologiques imprévus, inhabituels et extrêmes. Il s'agit notamment des températures extrêmes, des sécheresses, des fortes précipitations, des orages, de la pluie verglaçante, de la neige, des cycles de gel-dégel changeants, du givre, de la grêle, des vents violents et des tornades. Cela peut avoir d'autres conséquences, telles que l'élévation du niveau de la mer et des sécheresses intenses, qui menacent les cultures, la faune et les réserves d'eau douce. Voici quelques exemples tirés de mon expérience dans le domaine des transports ferroviaires publics qui sont désormais courants : nos voies ferrées et nos lignes de bus...

3 janvier 2018 - Forum économique mondial : Deux degrés de transformation
Les entreprises s'unissent pour lutter contre le changement climatique. Vous joindrez-vous à elles ?

4 Extrait de Wikipédia - https://en.wikipedia.org/wiki/Climate_change_adaptation

Chart #2

Risk categories	2 years
Economic	1st Misinformation and disinformation
Environmental	2nd Extreme weather events
Geopolitical	3rd State-based armed conflict
Societal	4th Societal polarization
Technological	5th Cyber espionage and warfare
	6th Pollution
	7th Inequality
	8th Involuntary migration or displacement
	9th Geoeconomic confrontation
	10th Erosion of human rights and/or civic freedoms

Source
World Economic Forum
Global Risks
Perception Survey 2024-2025

Graphique n° 2

10 years
1st Extreme weather events
2nd Biodiversity loss and ecosystem collapse
3rd Critical change to Earth systems
4th Natural resource shortages
5th Misinformation and disinformation
6th Adverse outcomes of AI technologies
7th Inequality
8th Societal polarization
9th Cyber espionage and warfare
10th Pollution

Source
Forum économique mondial
Risques mondiaux
Enquête de perception
2024-2025

in Davos Switzerland in 2019, extreme weather failed climate change mitigation, and natural disasters are the top five risks they face (see chart 2). The World Economic Forum presented this at its annual summit in Davos. (https://www.weforum.org/focus/davos-2019). As well as the World Economic Forum's Global Risk report (2019).

Context/ Terminology

Here are some business continuity definitions to provide context for this paper:

- **Business Continuity Management (BCM)** is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities. (Source: ISO 22301)
- **Business Continuity (BC)** is the ability of an organization to ensure continuity of service and support for its customers and to maintain its viability before, after, and during an event (Source ISO 22301). It is what needs to be done by an organization to ensure that essential functions can continue during and after a disaster, including preventing interruption of mission-critical services and reestablishing full functioning as quickly as possible.
- **Business Continuity Planning** is developing advanced arrangements and procedures that enable an organization to respond to an event so that critical business functions continue with minimal disruption or resume within planned levels of interruption.
- **A Business Continuity Plan (BCP)** is a document with advanced arrangements and procedures

Les organisations prennent conscience des dangers posés par le changement climatique et les conditions météorologiques extrêmes. Les évaluations climatiques et environnementales continuent de les classer parmi les risques dominants. Selon les PDG du monde entier interrogés dans le cadre d'un rapport du Forum économique mondial présenté à Davos, en Suisse, en 2019, les conditions météorologiques extrêmes ont fait échouer les efforts d'atténuation du changement climatique, et les catastrophes naturelles figurent parmi les cinq principaux risques auxquels ils sont confrontés (voir graphique 2). Le Forum économique mondial a présenté ces résultats lors de son sommet annuel à Davos. (https://www.weforum.org/focus/davos-2019). Ainsi que dans le rapport sur les risques mondiaux du Forum économique mondial (2019).

Contexte/Terminologie

Voici quelques définitions relatives à la continuité des activités afin de contextualiser le présent document :

- **La gestion de la continuité des activités (GCA)** est un processus de gestion holistique qui identifie les impacts potentiels menaçant une organisation et fournit un cadre pour renforcer la résilience et la capacité à réagir efficacement afin de protéger les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités créatrices de valeur. (Source : ISO 22301)

- **La continuité des activités (BC)** est la capacité d'une organisation à assurer la continuité du service et du soutien à ses clients et à maintenir sa viabilité avant, après et pendant un événement (Source ISO 22301). Il s'agit de ce qu'une organisation doit faire pour garantir la continuité des fonctions essentielles pendant et après une catastrophe, notamment en empêchant l'interruption des services critiques et en rétablissant le fonctionnement complet le plus rapidement possible.

- **La planification de la continuité des activités** consiste à élaborer des dispositions et des procédures avancées qui permettent à une organisation de réagir à un événement afin que les fonctions commerciales essentielles se poursuivent avec un minimum de perturbations ou reprennent dans les limites prévues.

that enable an organization to respond to an event so that critical business functions continue with planned levels of interruption or essential change.

- **A disaster,** for BCM purposes, is a sudden, unplanned catastrophic event causing significant damage or loss. It can be an event that creates an inability on an organization's part to provide critical business functions for some predetermined period. In the business environment, a disaster is any event that prevents an organization from providing essential business functions for some predetermined period. The disaster period begins when company management diverts from normal production responses and exercises its disaster recovery plan, sometimes moving from a primary to an alternate location.

Integrating Practices

By integrating BCM, ERM, and climate change sustainability practices (CCSP), you can build an essential platform to prioritize sustainability risks and mitigation responses for short- and long-term contingencies.

Adaptation, adaptive capacity, and vulnerability is "A conversation about climate resilience is incomplete without incorporating the concepts of adaptations, vulnerability, and climate change. If the definition of resiliency is the ability to recover from a negative event, in this case, climate change, then

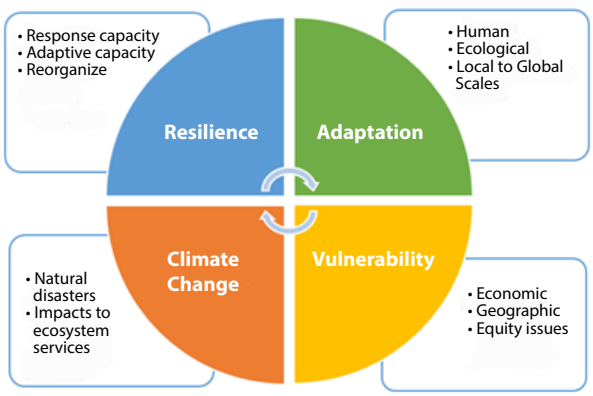
- **Un plan de continuité des activités (PCA)** est un document contenant des dispositions et des procédures avancées qui permettent à une organisation de réagir à un événement afin que les fonctions commerciales essentielles se poursuivent avec un niveau d'interruption ou de changement essentiel prévu.

- Dans le cadre de la gestion de la continuité des activités, **une catastrophe** est un événement soudain et imprévu qui cause des dommages ou des pertes importants. Il peut s'agir d'un événement qui empêche une organisation d'assurer ses fonctions commerciales essentielles pendant une période prédéterminée. Dans le monde des affaires, une catastrophe est tout événement qui empêche une organisation d'assurer ses fonctions commerciales essentielles pendant une période prédéterminée. La période de catastrophe commence lorsque la direction de l'entreprise s'écarte des réponses de production normales et met en œuvre son plan de reprise après sinistre, parfois en déménageant d'un site principal vers un site alternatif.

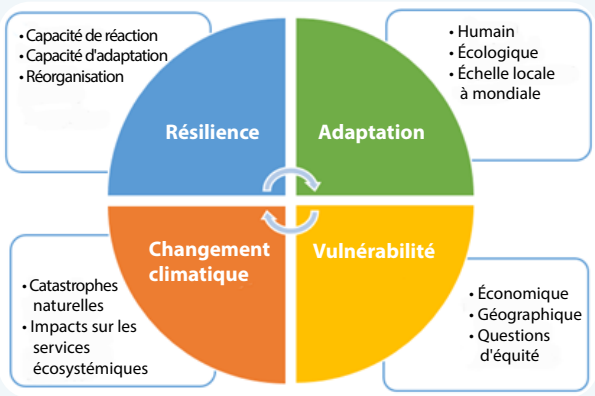
Intégration des pratiques

En intégrant les pratiques de BCM, d'ERM et de durabilité face au changement climatique (CCSP), vous pouvez créer une plateforme essentielle pour hiérarchiser les risques liés à la durabilité et les mesures d'atténuation pour les imprévus à court et à long terme.

Chart #3



Graphique n° 3



talking about preparations beforehand and strategies for recovery (aka adaptations), as well as populations that are less capable of developing and implementing a resiliency strategy (aka vulnerable populations), are essential. This is framed under the assumed detrimental impacts of climate change to ecosystems and ecosystem services ."[5]

Business Continuity Planning

"Batten down the hatches" is a nautical term that gives the order to secure a ship's hatch-tarpaulins when rough weather is expected. This closes the doors to the outside, as a protection against bad weather. One can do the same for a business before extreme weather like hurricanes. Business Continuity Planning is proactive and can prepare an organization with timely responses to incidents and threats of concern.

BCM follows standards that are fundamental in its delivery framework. One such measure, ISO22301, BCM, includes identifying potential threats and analyzing possible impacts to the organization, planning for and taking steps to build operational resilience and capacity to deal with unforeseen incidents that can affect an organization's ability to deliver its products and services to all users. Business continuity is deemed a risk control, as response plans mitigate disruptions to people, processes, and technology. The plan–do–check–act cycle is a four-step model for ensuring that the lessons learned from a previous event become embedded in standard operating procedures. Business continuity planning has no end, as the process is repeated for continuous improvement.

Institutionalizing BCM Governance Policy and Program Management (like the one in chart #4) promotes the development of appropriate response plans that are comprehensive, focused, and operable. Leveraging an "all-hazard, risk-based planning

[5] Smit, Barry, and Johanna Wandel. "Adaptation, adaptive capacity and vulnerability." Global environmental change 16.3 (2006): 282–292.

Adaptation, capacité d'adaptation et vulnérabilité : « Une conversation sur la résilience climatique est incomplète si elle n'intègre pas les concepts d'adaptation, de vulnérabilité et de changement climatique. Si la résilience se définit comme la capacité à se remettre d'un événement négatif, en l'occurrence le changement climatique, il est alors essentiel de parler des préparatifs préalables et des stratégies de reprise (alias adaptations), ainsi que des populations moins aptes à élaborer et à mettre en œuvre une stratégie de résilience (alias populations vulnérables). Cela s'inscrit dans le cadre des effets néfastes supposés du changement climatique sur les écosystèmes et les services écosystémiques. » [5]

Planification de la continuité des activités

« Batten down the hatches » est un terme nautique qui désigne l'ordre de sécuriser les bâches des écoutilles d'un navire lorsque des conditions météorologiques difficiles sont prévues. Cela permet de fermer les portes vers l'extérieur, afin de se protéger contre les intempéries. On peut faire de même pour une entreprise avant des conditions météorologiques extrêmes telles que des ouragans. La planification de la continuité des activités est proactive et permet à une organisation de se préparer à réagir en temps opportun aux incidents et aux menaces préoccupants.

La BCM suit des normes fondamentales dans son cadre de mise en œuvre. L'une de ces mesures, la norme ISO 22301, BCM, comprend l'identification des menaces potentielles et l'analyse des impacts possibles sur l'organisation, la planification et la mise en place de mesures visant à renforcer la résilience opérationnelle et la capacité à faire face à des incidents imprévus qui peuvent affecter la capacité d'une organisation à fournir ses produits et services à tous les utilisateurs. La continuité des activités est

[5] Smit, Barry, et Johanna Wandel. « Adaptation, adaptive capacity and vulnerability » (Adaptation, capacité d'adaptation et vulnérabilité). Global environmental change 16.3 (2006) : 282-292.

Chart #4

approach" will address threats that pose the most significant risk to the business, regardless of cause. It focuses on the outcomes of events rather than the events themselves. This cycle involves compiling documentation, measuring and exercising effectiveness, conducting maintenance, and continually improving work.

The all-hazards approach is defined as documenting and implementing tasks and actions necessary to prepare for, respond to, and recover from the impacts of all types of risks. For example, loss of the workplace can be caused by any climatic parameter – including flood, hurricane, blizzard, or any other weather event. BCM planning does not mitigate the risk or occurrence but rather 'the consequence' of it. It is critical to know your business and identify time-sensitive work functions that must be recovered within 24 hours of a knockout and those that are integral to safety and security, operational integrity (what your customers have paid for and expect to receive), and the customer experience. Adaptive assessments of past events can show where capital should be invested to correct reoccurring impacts on business. For example, if a building was flooded, you could recommend mitigating the problem with structural repair or eliminating the risk by moving to a different location.

Graphique n° 4

considérée comme un contrôle des risques, car les plans d'intervention atténuent les perturbations pour les personnes, les processus et la technologie.

Le cycle « planifier-faire-vérifier-agir » est un modèle en quatre étapes qui permet de s'assurer que les leçons tirées d'un événement précédent sont intégrées dans les procédures opérationnelles standard. La planification de la continuité des activités n'a pas de fin, car le processus est répété dans le but d'une amélioration continue.

L'institutionnalisation de la politique de gouvernance et de la gestion des programmes de gestion de la continuité des activités (comme celle illustrée à la graphique n° 4) favorise l'élaboration de plans d'intervention appropriés, complets, ciblés et opérationnels. L'adoption d'une « approche de planification tous risques, fondée sur les risques » permettra de traiter les menaces qui présentent le risque le plus important pour l'entreprise, quelle qu'en soit la cause. Elle se concentre sur les conséquences des événements plutôt que sur les événements eux-mêmes. Ce cycle comprend la compilation de documents, la mesure et la mise en œuvre de l'efficacité, la maintenance et l'amélioration continue du travail.

L'approche tous risques consiste à documenter et à mettre en œuvre les tâches et les mesures nécessaires pour se préparer, réagir et se remettre des conséquences de tous types de risques. Par exemple, la perte du lieu de travail peut être causée par n'importe quel paramètre

Summarizing BCM Program Climate Change / Extreme Weather planning behaviors:

1. Core Planning Domains (address):
   - Operational Resilience (staff and process)
   - Information Resilience (technology)
   - Supply Chain Resilience (vendor capability)

2. Role Organizational Senior Leadership (and central to ensuring preparedness and capability)
   - Employee Behavior and Planning Excellence = Process Continuity and Reliability
   - Promotes overall client satisfaction during normal and abnormal operating conditions

3. BCM Program Structure and Methodology
   - All hazards approach
   - Considers impacts of extreme weather caused by climate change
   - Aligning with ISO22301: and best planning practices

4. Three (3) Lines of Defense model to build Business Continuity and resiliency capability
   - Business Continuity Management function in a governance Role (with qualified and certified staff)
   - Organizational Front-Line participation with planning, and
   - Partnered with Internal Audit, Enterprise Risk Management (ERM for validation), and your Sustainability, Planning, and Development office (or consultant).

Enterprise Risk Management (ERM)

Business risk is something that all organizations face and comes in many types. It is essential to

climatique, notamment une inondation, un ouragan, une tempête de neige ou tout autre événement météorologique. La planification de la gestion de la continuité des activités (BCM) ne réduit pas le risque ou la survenue, mais plutôt « les conséquences » de celui-ci. Il est essentiel de connaître votre entreprise et d'identifier les fonctions de travail urgentes qui doivent être rétablies dans les 24 heures suivant une panne, ainsi que celles qui sont essentielles à la sûreté et à la sécurité, à l'intégrité opérationnelle (ce pour quoi vos clients ont payé et ce qu'ils s'attendent à recevoir) et à l'expérience client. Des évaluations adaptatives des événements passés peuvent montrer où il convient d'investir des capitaux pour corriger les impacts récurrents sur l'activité. Par exemple, si un bâtiment a été inondé, vous pouvez recommander d'atténuer le problème par des réparations structurelles ou d'éliminer le risque en déménageant dans un autre endroit.

Résumé des comportements de planification du programme BCM en matière de changement climatique et de conditions météorologiques extrêmes :

1. Domaines de planification fondamentaux (adresse) :
   - Résilience opérationnelle (personnel et processus)
   - Résilience de l'information (technologie)
   - Résilience de la chaîne d'approvisionnement (capacité des fournisseurs)

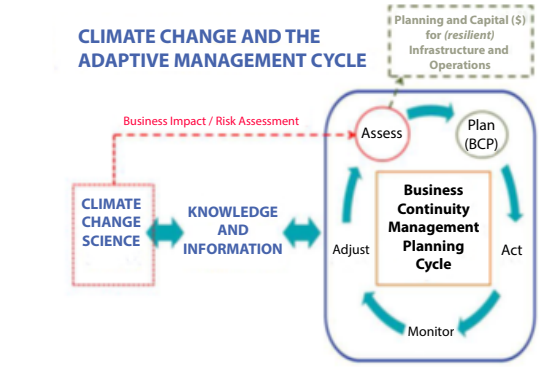
2. Rôle de la haute direction de l'organisation (essentiel pour garantir la préparation et la capacité)
   - Comportement des employés et excellence de la planification = continuité et fiabilité des processus

- Favorise la satisfaction globale des clients dans des conditions d'exploitation normales et anormales

3. Structure et méthodologie du programme BCM
   - Approche tous risques
   - Prend en compte les impacts des conditions météorologiques extrêmes causées par le changement climatique
   - Alignement sur la norme ISO22301 et les meilleures pratiques de planification

4. Modèle à trois (3) lignes de défense pour renforcer la continuité des activités et la capacité de résilience
   - Fonction de gestion de la continuité des activités dans un rôle de gouvernance (avec un personnel qualifié et certifié)

Chart #5



identify, rank, rate, and quantify risk so that adequate mitigation plans are in place to deal with it. In my practice and experience, the identification, assessment, and prioritization of risks is followed by implemented 'controls' to minimize, monitor, and control the risk's probability and impact (or to maximize the realization of opportunities). Risk actions, as we have come to know, include:

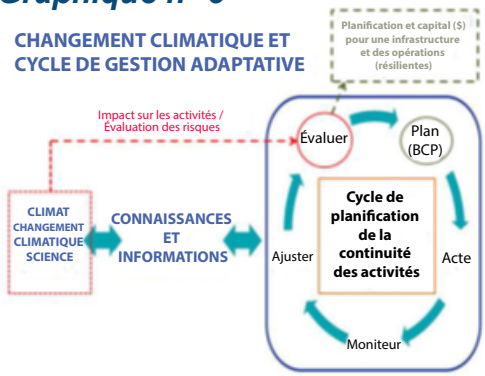
- Acceptance (we can accept and live with it);
- Elimination (if we do this, it won't happen);
- Mitigation (if we do this, it won't be so bad); and
- Transfer (shifted to another 3rd party, typically an insurer or new owner).

Risk controls are actions to reduce or eliminate risks identified proactively. The greater the risk control capability (n+1) – the greater the cost. BCM itself is deemed a risk control that can manage the risk by building response plans or physical diversity or redundancy with facilities, operations, and the workplace

An enterprise risk management program plays a vital role in the surveillance, monitoring, and management of risks and opportunities. For example, ISO 31000 (see figure XX) offers a defined evaluation process that can help guide organizations through the identification of threats and planning for risk treatment.

The Canadian Climate Change Risk Assessment Guide (A Strategic Overview of Climate Risks and Their Impact on Organizations (Interim Version June 2014) is a guide written to assist small- and medium-

Graphique n° 5



- Participation de la première ligne de l'organisation à la planification, et
- Partenariat avec l'audit interne, la gestion des risques d'entreprise (ERM pour la validation) et votre bureau (ou consultant) chargé de la durabilité, de la planification et du développement.

Gestion des risques d'entreprise (ERM)

Les risques commerciaux sont une réalité à laquelle toutes les organisations sont confrontées et qui se présente sous de nombreuses formes. Il est essentiel d'identifier, de classer, d'évaluer et de quantifier les risques afin de mettre en place des plans d'atténuation adéquats pour y faire face. D'après ma pratique et mon expérience, l'identification, l'évaluation et la hiérarchisation des risques sont suivies de la mise en œuvre de « contrôles » visant à minimiser, surveiller et contrôler la probabilité et l'impact des risques (ou à maximiser la concrétisation des opportunités). Les mesures de gestion des risques, comme nous le savons, comprennent :

- L'acceptation (nous pouvons l'accepter et vivre avec) ;
- L'élimination (si nous faisons cela, cela ne se produira pas) ;
- L'atténuation (si nous faisons cela, ce ne sera pas si grave) ; et
- Le transfert (transféré à un tiers, généralement un assureur ou un nouveau propriétaire).

Les contrôles des risques sont des mesures visant à réduire ou à éliminer les risques identifiés de manière proactive. Plus la capacité de contrôle des risques (n+1) est

sized organizations in understanding the risks and opportunities of climate impacts and how to manage them[6]. The Guide can be found at: https://www.iclr.org/wp-content/uploads/PDFS/CC_Risk_Assessment_Guide_Interim2_Jun_8_14_.pdf

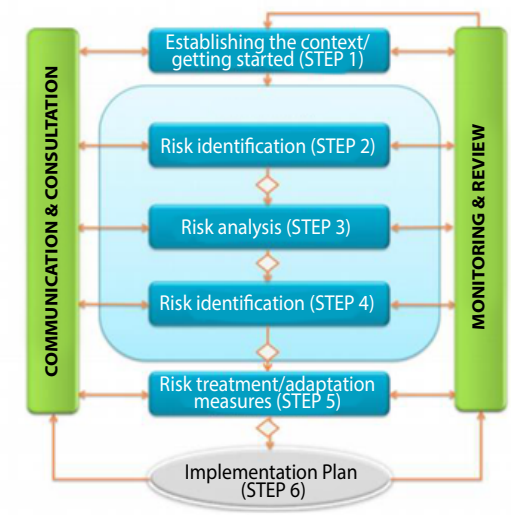
Engineers Canada has developed more technical approaches to Risk management and climate change impacts. It is known as The Public, Infrastructure, Engineering, Vulnerability, and Committee (PIEVC) has created a protocol to assess the vulnerability of infrastructure to extreme weather events and future climate changes. This enables better planning and design and climate-resilient infrastructure. For information, reference PIEVC at https://pievc.ca/protocol/

Conclusion

Climate change and extreme weather represent a known risk. Companies that experienced business interruptions due to severe weather experienced a loss of revenue and customer confidence. While the numbers can be quantified, insured damage for extreme weather events across Canada in 2018 reached $1.9 billion[7], the more significant threat is that many unprepared businesses run the compounded risk of never really recovering.

Chart #6

THE ISO31000 RISK MANAGEMENT PROCESS



[6] Summary from the Canadian Climate Change Risk Assessment Guide.

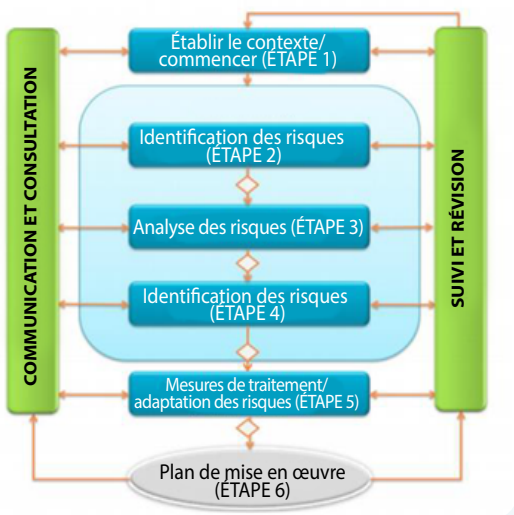
grande, plus le coût est élevé. La gestion de la continuité des activités (GCA) est elle-même considérée comme un contrôle des risques qui permet de gérer les risques en élaborant des plans d'intervention ou en mettant en place une diversité physique ou une redondance au niveau des installations, des opérations et du lieu de travail

Un programme de gestion des risques d'entreprise joue un rôle essentiel dans la surveillance, le suivi et la gestion des risques et des opportunités. Par exemple, la norme ISO 31000 (voir figure XX) propose un processus d'évaluation défini qui peut aider les organisations à identifier les menaces et à planifier le traitement des risques.

Le Guide canadien d'évaluation des risques liés aux changements climatiques (Aperçu stratégique des risques climatiques et de leur incidence sur les organisations (version provisoire de juin 2014) est un guide rédigé pour aider les petites et moyennes organisations à comprendre les risques et les opportunités liés aux impacts climatiques et à les gérer[6]. Le guide est disponible à l'adresse suivante : https://www.iclr.org/wp-content/uploads/PDFS/CC_Risk_Assessment_Guide_Interim2_Jun_8_14_.pdf

Graphique n° 6

LE PROCESSUS DE GESTION DES RISQUES ISO 31000



[6] Résumé tiré du Guide canadien d'évaluation des risques liés aux changements climatiques.

A structured approach to Business Continuity Management should focus on operational processes, functions, and supporting technology. It must also identify strategies to help the business survive a disaster and deliver mission-critical services. Scenarios to consider planning for include the following:

- Your office building or manufacturing facility is unavailable, damaged, or destroyed.
- Operational staff and management are unavailable for extended periods.
- Power and other utilities become unavailable or intermittent; or
- The supply chain is interrupted.

Planning for a hurricane or any other risk event impacting your

Ingénieurs Canada a élaboré des approches plus techniques en matière de gestion des risques et des impacts du changement climatique. Le Comité sur les infrastructures publiques, l'ingénierie et la vulnérabilité (PIEVC) a créé un protocole pour évaluer la vulnérabilité des infrastructures aux phénomènes météorologiques extrêmes et aux changements climatiques futurs. Cela permet une meilleure planification et conception d'infrastructures résilientes au climat. Pour plus d'informations, consultez le site du PIEVC à l'adresse https://pievc.ca/protocol/.

Conclusion

Le changement climatique et les conditions météorologiques extrêmes représentent un risque connu. Les entreprises qui ont subi des interruptions d'activité en raison de conditions météorologiques extrêmes ont enregistré une perte de revenus et une baisse de confiance de la part de leurs clients. Si les chiffres peuvent être quantifiés, les dommages assurés liés aux événements météorologiques extrêmes au Canada en 2018 ont atteint 1,9 milliard de dollars[7], la menace la plus importante réside dans le fait que de nombreuses entreprises non préparées courent le risque accru de ne jamais vraiment se remettre de ces événements.

Une approche structurée de la gestion de la continuité des activités doit se concentrer sur les processus opérationnels, les fonctions et les technologies de soutien. Elle doit également identifier des stratégies pour aider l'entreprise

business is a good business practice. It is not always about plans and processes; it must include organizational culture within the company. Agility can be seen as forethought and is crucial as the best-prepared plan may have its challenges when activated under duress conditions. Are you prepared for the next significant event impacting your business? Operational resiliency to the impacts of severe weather caused by climate change is a destination; Business Continuity Management can take you there.

- Where to start? Risk Based Approach, know what you have and prioritize by risk
- Learn from lessons learned, as you cannot predict a disaster, but you can plan for one. Ω

ABOUT THE AUTHOR

Vito Mangialardi *is an international award-winning Senior Manager and Operational Resiliency expert specializing in LEAN practices. He bridges the gap between complex project delivery and organizational health, protecting people, processes, and technology from disruption. Currently an independent consultant and "go-to expert" for business continuity. Vito is leading his own practice in building empowered, customer-centric cultures that transform operational risk into strategic endurance. Vito's leadership with planning in desired outcomes focuses on challenging the status quo—identifying effective recovery strategies, not just easy—to ensure the integrity of the brand (products or services) and the continuity of the organization in meeting customer/user expectations.*

[7] Catastrophe Indices and Quantification Inc. January 16, 2019 (OTTAWA)

à survivre à une catastrophe et à fournir des services essentiels à sa mission. Les scénarios à prendre en compte dans la planification sont les suivants :

- Votre immeuble de bureaux ou votre site de production est indisponible, endommagé ou détruit.
- Le personnel opérationnel et la direction sont indisponibles pendant de longues périodes.
- L'électricité et les autres services publics deviennent indisponibles ou intermittents ; ou
- La chaîne d'approvisionnement est interrompue.

Il est bon pour une entreprise de se préparer à un ouragan ou à tout autre événement risqué pouvant avoir un impact sur ses activités. Il ne s'agit pas toujours de plans et de processus ; cela doit inclure la culture organisationnelle au sein de l'entreprise. L'agilité peut être considérée comme de la prévoyance et est cruciale, car même le plan le mieux préparé peut rencontrer des difficultés lorsqu'il est mis en œuvre dans des conditions difficiles. Êtes-vous prêt à faire face au prochain événement majeur qui affectera votre entreprise ? La résilience opérationnelle face aux effets des conditions météorologiques extrêmes causées par le changement climatique est un objectif ; la gestion de la continuité des activités peut vous y aider.

- Par où commencer ? Adoptez une approche basée sur les risques, identifiez vos atouts et établissez des priorités en fonction des risques.
- Tirez les leçons du passé, car vous ne pouvez pas prédire une catastrophe, mais vous pouvez vous y préparer. Ω

À PROPOS DE L'AUTEUR

Vito Mangialardi est un cadre supérieur primé à l'échelle internationale et un expert en résilience opérationnelle spécialisé dans les pratiques LEAN. Il comble le fossé entre la réalisation de projets complexes et la santé organisationnelle, protégeant les personnes, les processus et la technologie contre les perturbations. Actuellement consultant indépendant et « expert incontournable » en matière de continuité des activités, Vito dirige son propre cabinet et s'attache à créer des cultures autonomes et centrées sur le client qui transforment le risque opérationnel en endurance stratégique. Le leadership de Vito en matière de planification des résultats souhaités consiste à remettre en question le statu quo, en identifiant des stratégies de reprise efficaces, et pas seulement faciles, afin de garantir l'intégrité de la marque (produits ou services) et la continuité de l'organisation dans la satisfaction des attentes des clients/utilisateurs.

[7] Catastrophe Indices and Quantification Inc. 16 janvier 2019 (OTTAWA)

Letters to the Editor

Lettres à la rédaction

In this edition of True North Resilience, we've had the idea to introduce a section for "Letters to the Editor." The intent behind introducing such a section is simple: resilience is not a static discipline. Rather, it benefits from dialogue just as much as it does from expertise. While articles and research provide structure and insight as to new ideas, we believe that it is often through informed reflection and respectful challenge based on shared experience that our thinking can truly evolve.

This new section is meant to create space for us as professionals to engage with ideas presented in our publication. It is a section to agree, disagree, expand, or reframe thoughts based on lived experience. In this field defined by uncertainty and adaptation, I personally believe thoughtful discourse is not a distraction from resilience; it is a core component of it.

We hope this feature encourages constructive debate, and a deeper sense of community across our profession. After all, community is what we are trying to build & reinforce.

- Alexander Landry, P.Eng., PMP, CBCP

Dans cette édition de True North Resilience, nous avons eu l'idée d'introduire une section intitulée « Lettres à la rédaction ». L'intention derrière l'introduction d'une telle section est simple : la résilience n'est pas une discipline statique. Elle tire autant profit du dialogue que de l'expertise. Si les articles et les recherches fournissent une structure et un aperçu des nouvelles idées, nous pensons que c'est souvent grâce à une réflexion éclairée et à une remise en question respectueuse fondée sur des expériences partagées que notre pensée peut véritablement évoluer.

Cette nouvelle rubrique vise à créer un espace où nous, professionnels, pouvons échanger sur les idées présentées dans notre publication. Il s'agit d'une rubrique où l'on peut approuver, désapprouver, développer ou recadrer des réflexions basées sur des expériences vécues. Dans ce domaine caractérisé par l'incertitude et l'adaptation, je pense personnellement qu'un discours réfléchi n'est pas une distraction par rapport à la résilience, mais qu'il en est un élément central.

Nous espérons que cette rubrique encouragera un débat constructif et un sentiment d'appartenance plus profond à notre profession. Après tout, c'est une communauté que nous essayons de construire et de renforcer.

- Alexander Landry, P.Eng., PMP, CBCP

Letter to the Editor:

Old Man Yells at Cloud

By ***Kevin Powers***

First came the Mainframe, a central computer that handled the entire workload. Then came the desktop PC - computing could now happen locally. After that came the client/server model with desktop PCs connecting to in house server farms. Next was the Internet, a distributed worldwide network, and now… Now we have a centralized infrastructure where the distributed worldwide internet has been bought and sold into a limited number of cloud services.

There has been a bigger push in recent years, whether by decision or by being "voluntold" by vendors, to move to cloud service. It was promised as a cost saving move, cutting back on costly in-house server farms and per person costs to maintain those servers. We (the IT world) were promised five 9's (99.999%) of uptime, and that it would have redundancies. Everything would be fine.

More services, websites, and server infrastructure were moved to the cloud and into these massive datacentres, owned by a handful of companies, in particular, Amazon and Microsoft[1] Despite the promises of redundancy, we have seen firsthand that the datacentres are a single point of failure. The Amazon Web Services (AWS) outage on October 20th clearly indicated that one datacentre going down can in fact cripple a large portion of the internet. Despite multiple datacentres around the world, the root cause of the AWS outage was a "problematic update" to a core managed database service. This triggered failures in the Domain Name System (DNS). Without DNS the translation from a website address to the actual IP address, causing services and website to

Lettre à la rédaction :

Un vieil homme crie sur le cloud

Par ***Kevin Powers***

Il y a d'abord eu le Mainframe, un ordinateur central qui gérait l'ensemble de la charge de travail. Puis vint l'ordinateur de bureau : l'informatique pouvait désormais s'effectuer localement. Ensuite est apparu le modèle client/serveur, avec des PC de bureau connectés à des fermes de serveurs internes. Puis est venu Internet, un réseau mondial distribué, et maintenant... Nous disposons désormais d'une infrastructure centralisée où l'Internet mondial distribué a été acheté et vendu sous forme d'un nombre limité de services cloud.

Ces dernières années, on a assisté à une forte poussée, qu'elle soit volontaire ou imposée par les fournisseurs, vers les services cloud. On nous a promis des économies, grâce à la suppression des coûteuses fermes de serveurs internes et des frais par personne liés à la maintenance de ces serveurs. On nous a promis (à nous, le monde informatique) une disponibilité de 99,999 % et des redondances. Tout irait bien.

De plus en plus de services, de sites web et d'infrastructures serveurs ont été transférés vers le cloud et vers ces immenses centres de données, détenus par une poignée d'entreprises, notamment, Amazon et Microsoft[1]. Malgré les promesses de redondance, nous avons pu constater de nos propres yeux que les centres de données constituent un point de défaillance unique. La panne d'Amazon Web Services (AWS) survenue le 20 octobre a clairement montré qu'un seul centre de données en panne peut en réalité paralyser une grande partie de l'internet. Malgré la présence de multiples centres de données à travers le monde, la cause première de la panne d'AWS était une « mise à jour problématique » d'un service de base de données géré centralisé. Cela a déclenché des défaillances dans

[1] https://www.blackridgeresearch.com/blog/list-top-largest-biggest-data-center-providers-companies-in-the-world#toc-0-list-of-top-10-largest-data-center-companies-in-the-world

become unavailable. This caused critical AWS infrastructure to fail taking down 113 AWS services[2].

Despite being taught a valuable lesson, Microsoft was determined to make headlines less than two weeks later on October 29th. In this case a change was made to the Azure load-balancing and content-delivery service, it cascaded and resulted in major Microsoft services being unavailable. Including Microsoft 365 (formerly Office 365). Coincidentally, Microsoft had ended support and updates for Office 2016 and 2019 on October 14th. The logical move was to Microsoft 365 to take advantage of regular updates and cloud-based storage solutions. IT departments around the globe were left saying "nothing we can do", and no amount of C-Suite yelling will change that.

With IT departments still recovering from being in the line of fire for someone to blame, less than a month later on November 18th Cloudflare had a near 6-hour outage. Cloudflare is one of the most prominent DNS providers. They have a layer of security on top of their DNS services to help prevent some malicious behaviour[3]. With DNS unavailable across the internet, this wasn't impactful to just one provider (such as the Azure outage) but to the entire Internet at large.

In my day-to-day role of managing a 1st and 2nd level support team, I heard a lot about the outages and fortunately most people I spoke with understood that it was not us. Having it reported on the major news networks helps. Fortunately, due to the scope of the outages practically every other company was dealing with the same issues. While there is no number that I could find and confirm, Forbes cites **Mehdi Daoudi**, the CEO of Catchpoint, indicating that the AWS outage could reach into the hundreds of billions from lost productivity[4].

le système de noms de domaine (DNS). Sans DNS, la traduction d'une adresse de site web en adresse IP réelle n'est plus possible, rendant les services et les sites web indisponibles. Cela a entraîné la défaillance de l'infrastructure critique d'AWS, mettant hors service 113 services AWS[2]

Malgré cette précieuse leçon, Microsoft était déterminé à faire la une des journaux moins de deux semaines plus tard, le 29 octobre. Dans ce cas, une modification a été apportée au service Azure de répartition de charge et de diffusion de contenu, ce qui a entraîné une cascade de problèmes et rendu indisponibles plusieurs services Microsoft majeurs, dont Microsoft 365 (anciennement Office 365). Par coïncidence, Microsoft avait mis fin au support et aux mises à jour pour Office 2016 et 2019 le 14 octobre. La décision logique était de passer à Microsoft 365 pour profiter des mises à jour régulières et des solutions de stockage dans le cloud. Les services informatiques du monde entier se sont retrouvés dans l'impuissance, et aucune protestation de la part des dirigeants n'y changera quoi que ce soit.

Alors que les services informatiques se remettaient à peine d'avoir été pris pour cible, moins d'un mois plus tard, le 18 novembre, Cloudflare a subi une panne de près de 6 heures. Cloudflare est l'un des fournisseurs DNS les plus importants. Il dispose d'une couche de sécurité en plus de ses services DNS afin de prévenir certains comportements malveillants[3]. L'indisponibilité du DNS sur Internet n'a pas eu d'impact sur un seul fournisseur (comme dans le cas de la panne d'Azure), mais sur l'ensemble de l'Internet.

Dans le cadre de mes fonctions quotidiennes de gestion d'une équipe d'assistance de premier et deuxième niveaux, j'ai beaucoup entendu parler des pannes et, heureusement, la plupart des personnes à qui j'ai parlé ont compris que cela ne venait pas de nous. Le fait que les principaux réseaux d'information en aient fait état a aidé. Heureusement, en

[2] https://dev.to/cloud_man/the-aws-outage-of-october-20-2025-what-happened-who-was-affected-and-lessons-learned-5b35

[3] https://dn.org/top-dns-service-providers-in-2025-comprehensive-review-and-ranking-of-leading-dns-providers/

[4] https://www.forbes.com/sites/christerholloman/2025/10/20/aws-outage-billions-lost-multi-cloud-is-wall-streets-solution/

I also know that Daoudi's publication is focused on disaster recovery, something I will not claim to have more than a "best effort" of understanding of. I know the fundamentals and I know that having a documented plan is a requirement. It falls apart when the outage is global and not something we can control. It's easy to move to an offsite datacentre, move our in-house services over and bring our organization back up. However, that is a moot point when the software and services we rely on are cloud based and inaccessible.

I have been at this a long time, both professionally and personally, and despite the promises told of the Internet in the 90's we have failed to properly keep it as a distributed network, allowing a handful of major companies to consolidate and control most of the infrastructure of the world. Call me paranoid, but I am the old man yelling at a cloud (Simpsons reference). I respect the need for cloud-based solutions and compute power, however when we rely on them exclusively, we are opening ourselves up to an impossible to plan for disaster that in all fairness relies on those companies' disaster recovery plans. Not to get too far into conspiracy theories, but it also highlights how taking out one piece of the puzzle can cripple the world. Ω

raison de l'ampleur des pannes, pratiquement toutes les autres entreprises étaient confrontées aux mêmes problèmes. Bien que je n'aie trouvé aucun chiffre que je puisse confirmer, Forbes cite **Mehdi Daoudi**, PDG de Catchpoint, qui indique que la panne d'AWS pourrait entraîner des pertes de productivité se chiffrant en centaines de milliards[4].

Je sais également que la publication de Daoudi porte principalement sur la reprise après sinistre, un domaine que je ne prétends pas maîtriser parfaitement. J'en connais les principes fondamentaux et je sais qu'il est indispensable de disposer d'un plan documenté. Mais cela ne fonctionne pas lorsque la panne est mondiale et hors de notre contrôle. Il est facile de déménager dans un centre de données hors site, d'y transférer nos services internes et de remettre notre organisation sur pied. Cependant, cela n'a aucun sens lorsque les logiciels et les services sur lesquels nous comptons sont basés sur le cloud et inaccessibles.

Je travaille dans ce domaine depuis longtemps, tant sur le plan professionnel que personnel, et malgré les promesses faites au sujet d'Internet dans les années 90, nous n'avons pas réussi à le maintenir correctement en tant que réseau distribué, permettant à une poignée de grandes entreprises de consolider et de contrôler la majeure partie de l'infrastructure mondiale. Traitez-moi de paranoïaque, mais je suis le vieil homme qui crie sur un nuage (référence aux Simpsons). Je respecte le besoin de solutions basées sur le cloud et de puissance de calcul, mais lorsque nous nous appuyons exclusivement sur elles, nous nous exposons à une catastrophe impossible à prévoir qui, en toute honnêteté, dépend des plans de reprise après sinistre de ces entreprises. Sans vouloir trop m'aventurer dans les théories du complot, cela montre également à quel point le retrait d'une seule pièce du puzzle peut paralyser le monde. Ω

ABOUT THE AUTHOR

***Kevin Powers** is a seasoned IT leader with over 20 years of experience supporting a prominent Bay Street law firm in Toronto, an avid shade-tree mechanic, and an advocate for those with Down syndrome.*

À PROPOS DE L'AUTEUR

***Kevin Powers** est un leader chevronné en TI avec plus de 20 ans d'expérience dans le soutien d'un important cabinet d'avocats de Bay Street à Toronto, un fervent mécanicien d'arbres d'ombrage et un défenseur des personnes atteintes du syndrome de Down.*

Four Years Later

How Michael Taylor Intends to Evolve Resilience at Felder Corporation

Quatre ans plus tard

Comment Michael Taylor entend développer la résilience chez Felder Corporation

By/Par **Brian Zawanda**

Four years ago, I published a book titled "*The Business Continuity Operating System – What the Best Do Differently to Achieve Success.*"

It wasn't a textbook.
It was a business fable.

The story followed Michael Taylor, a newly appointed continuity leader at a fictitious manufacturing company called The Felder Corporation, as he worked to build something most organizations said they wanted—but rarely achieved: a business continuity program that delivered appropriate continuity/resilience capability.

At the time, Michael's challenge was familiar:

- Siloed risk ownership
- Business continuity treated as a compliance exercise
- Success measured by document completion rather than operational confidence

The solution, then, was a system: governance, ownership, lifecycle management, and executive alignment.

It worked. Much of it still does because there is a core focus on engagement, communication and capability.

But four years have passed...

Il y a quatre ans, j'ai publié un livre intitulé « *The Business Continuity Operating System – What the Best Do Differently to Achieve Success* » *(Le système d'exploitation de la continuité des activités – Ce que les meilleurs font différemment pour réussir).*

Ce n'était pas un manuel scolaire.
C'était une fable sur le monde des affaires.

L'histoire suivait Michael Taylor, un nouveau responsable de la continuité au sein d'une entreprise manufacturière fictive appelée The Felder Corporation, alors qu'il s'efforçait de mettre en place quelque chose que la plupart des organisations *disaient* vouloir, mais qu'elles obtenaient rarement : un programme de continuité des activités offrant une capacité de continuité/résilience appropriée.

À l›époque, le défi de Michael était familier :

- Responsabilité cloisonnée des risques
- La continuité des activités considérée comme un exercice de conformité
- Succès mesuré par l'achèvement des documents plutôt que par la confiance opérationnelle

La solution consistait donc en un *système* : gouvernance, responsabilité, gestion du cycle de vie et alignement des dirigeants.

Cela a fonctionné. Une grande partie fonctionne encore aujourd'hui, car l'accent est mis sur l'engagement, la communication et les capacités.

Mais quatre années se sont écoulées...

And the world — and Felder — has changed. Michael, and the Felder Corporation, is taking a step back to close a key gap, which is defining a holistic collection of availability, response and recovery controls to drive measurable resilience.

Back to Michael in his own words…

A Different Kind of Question

Over the holidays, while away from work, I couldn't help but think what I could do differently to provide a clearer ROI and get more efficient when it comes to driving higher levels of efficiency.

I started by asking myself, "if Felder and I were starting over *today*, would I have implemented the same approach?"

The answer is no — not because I was wrong at the time, but because the problem has evolved.

At Felder, we didn't fail at business continuity. Our organization simply matured during a challenging economic time, and our Board and customers now demand a program that delivers targeted capabilities. At the same time, because of resource demands, we needed to achieve higher levels of capability with a much a higher degree of efficiency.

Looking back four years, we did what many organizations do once they "get serious" about continuity and resilience:

- We defined resilience requirements heavily focused on response and recovery
- We documented plans that summarized how we would respond to a disruption
- We exercised to build skills and confidence
- We created risk registers to improve continuity and resilience
- We measured recoverability at a product/service level (KRIs) as well as if we performed key business continuity activities (KPIs)

At first, we were happy and confident, and we even responded well to a horrible

Et le monde — tout comme Felder — a changé. Michael et la Felder Corporation prennent du recul pour combler une lacune importante, à savoir la définition d'un ensemble holistique de contrôles de disponibilité, de réponse et de reprise afin de favoriser une résilience mesurable.

Revenons à Michael, selon ses propres mots...

Une question d'un autre genre

Pendant les vacances, loin du travail, je ne pouvais m'empêcher de réfléchir à ce que je pourrais faire différemment pour obtenir un retour sur investissement plus clair et gagner en efficacité afin d'atteindre des niveaux d'efficacité plus élevés.

J'ai commencé par me demander : « Si Felder et moi recommencions *aujourd'hui*, aurais-je mis en œuvre la même approche ? »

La réponse est non, non pas parce que j'avais tort à l›époque, mais parce que le problème a évolué.

Chez Felder, nous n'avons pas échoué en matière de continuité des activités. Notre organisation a simplement mûri pendant une période économique difficile, et notre conseil d'administration et nos clients exigent désormais un programme qui offre des capacités ciblées. Dans le même temps, en raison des besoins en ressources, nous devions atteindre des niveaux de capacité plus élevés avec un degré d'efficacité beaucoup plus important.

Avec quatre ans de recul, nous avons fait ce que font de nombreuses organisations lorsqu'elles se « sérieusement » penchent sur la continuité et la résilience :

- Nous avons défini des exigences en matière de résilience fortement axées sur la réponse et la reprise.
- Nous avons documenté des plans résumant la manière dont nous réagirions à une perturbation
- Nous avons mené des exercices pour développer nos compétences et notre confiance
- Nous avons créé des registres des risques afin d'améliorer la continuité et la résilience
- Nous avons mesuré la capacité de reprise au niveau des produits/services (KRI) ainsi que la mise en œuvre des activités clés de continuité des activités (KPI).

Au début, nous étions satisfaits et confiants, et nous avons même bien réagi à une terrible catastrophe na-

➤

natural disaster affecting our operations in Puerto Rico. But today, we're now looking to be better at preventing disruption and optimizing response and recovery processes.

Our executives are also starting to ask some important questions:

- "Which investments really improve resilience?"
- "Why do we keep debating likelihood when we all know it's a guess?"
- "How do we know we're getting better?"

That's when I came to this realization – Felder isn't suffering from a lack of risk identification. They were suffering from a lack of control clarity, meaning are we doing all we can pragmatically to prevent, respond to and recover from disruption. And it starts with defining the control set that needs to be applied through the organization then measuring effectiveness.

turelle qui a affecté nos opérations à Porto Rico. Mais aujourd'hui, nous cherchons à améliorer la prévention des perturbations et à optimiser les processus de réponse et de reprise.

Nos dirigeants commencent également à se poser des questions importantes :

- « Quels investissements améliorent réellement la résilience ? »
- « Pourquoi continuons-nous à débattre de la probabilité alors que nous savons tous qu›il s›agit d›une estimation ? »
- « Comment savoir si nous nous améliorons ? »

C'est alors que j'ai pris conscience d'une chose : Felder ne souffrait pas d'un manque d'identification des risques. L'entreprise souffrait d'un manque de clarté en matière de contrôle, c'est-à-dire que nous ne faisions pas tout notre possible de manière pragmatique pour prévenir les perturbations, y répondre et nous en remettre. Il faut donc commencer par définir l'ensemble des contrôles à appliquer au sein de l'organisation, puis mesurer leur efficacité.

C'est pourquoi nos efforts en 2026 se concentreront

That's why our efforts in 2026 will focus on answering this question – "What must be true for this business to continue operating under stress?"

Building on the results of the Frame Meeting we refreshed annually, meaning a focus on what to protect in terms of critical product/services and "how much" business continuity do we need, we will spend Q1 defining the controls that protect the organization's most critical assets, and how to assess if these controls are designed and operating effectively throughout Felder.

I don't intend to rip out what's in place but I do intend to evolve it. That evolution includes:

1. Beyond revisiting the Frame Meeting results, we will also revisit business impact analysis results, specifically reviewing and updating the collection of business processes and assets mapped to each in-scope product/service.
2. Then we will evaluate each dependent asset based on the availability, response, and recovery controls we identified. The controls will then be assessed for design and operational effectiveness. Weak controls create exposure. Strong controls reduce it. By prioritizing assets and their controls by the criticality associated with the critical business service they protect, a roadmap focused on continual improvement is realized.
3. Success is no longer "we did a BIA" or "we have a plan" but can we pragmatically prevent disruption and can we withstand disruption within our risk appetite? We will do this based on:
   - Assigning a criticality score to our products/services, processes and assets
   - Assigning a capability score to our products/services, processes

sur la réponse à cette question : « Que faut-il pour que cette entreprise continue à fonctionner dans des conditions difficiles ? »

En nous appuyant sur les résultats de la réunion-cadre que nous avons actualisée chaque année, c'est-à-dire en nous concentrant sur ce qu'il faut protéger en termes de produits/services essentiels et sur le « niveau » de continuité des activités dont nous avons besoin, nous passerons le premier trimestre à définir les contrôles qui protègent les actifs les plus critiques de l›organisation et à évaluer si ces contrôles sont conçus et fonctionnent efficacement dans l'ensemble de Felder.

Je n'ai pas l'intention de supprimer ce qui est en place, mais je souhaite le faire évoluer. Cette évolution comprend :

1. Au-delà de la révision des résultats de la réunion-cadre, nous réexaminerons également les résultats de l'analyse d'impact sur les activités, en particulier en révisant et en mettant à jour l'ensemble des processus et des actifs commerciaux associés à chaque produit/service concerné.
2. Nous évaluerons ensuite chaque actif dépendant en fonction des contrôles de disponibilité, de réponse et de récupération que nous avons identifiés. Les contrôles seront ensuite évalués en termes de conception et d›efficacité opérationnelle. Des contrôles faibles créent une exposition. Des contrôles solides la réduisent. En hiérarchisant les actifs et leurs contrôles en fonction de la criticité associée au service commercial critique qu'ils protègent, une feuille de route axée sur l'amélioration continue est mise en place.
3. Le succès ne se mesure plus à l›aune d›une « analyse d›impact sur les activités » ou d'un « plan », mais à notre capacité à prévenir de manière pragmatique les perturbations et à y résister dans les limites de notre appétit pour le risque. Pour ce faire, nous nous appuierons sur :
   - L'attribution d'un score de criticité à nos produits/services, processus et actifs
   - L'attribution d'un score de capacité à nos produits/services, processus et actifs en fonction de la conception et de l'efficacité opérationnelle des contrôles
   - Communiquer les scores de résilience aux risques et, si nécessaire, mettre en évidence les contrôles les plus faibles ayant la plus grande influence sur l'amélioration de notre score de résilience aux risques

and assets based on the design and operating effectiveness of controls
- Communicate resilience risk scores and where needed, highlight the weakest controls with the biggest influence on improving our resilience risk scoring

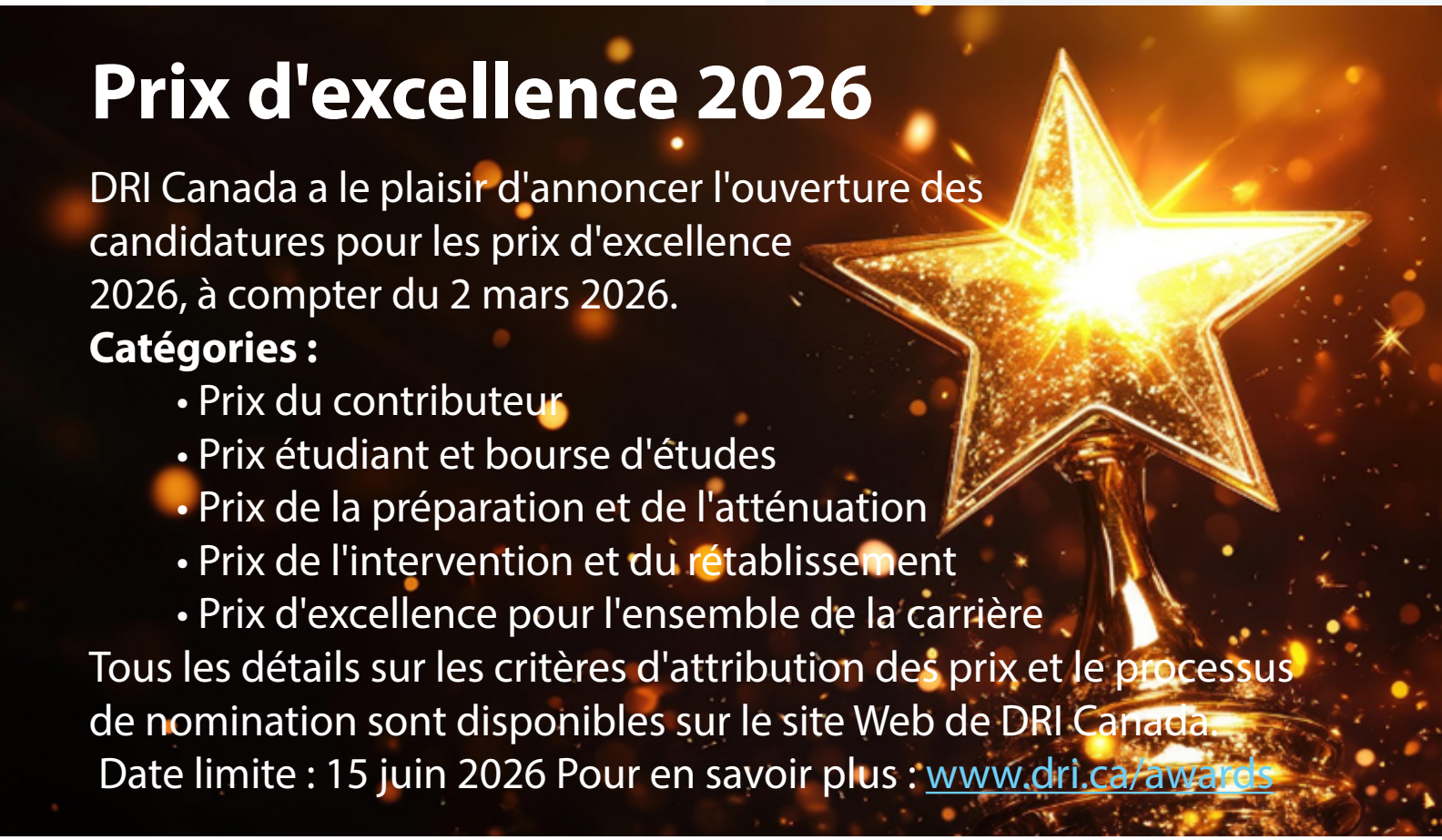
Four years ago, I measured success in seven important ways, and these value-adding elements persist today:

- Scoping through leadership discussion
- Documented continuity/resilience processes followed by all
- Clear roles with the right people participating
- Engagement at the right frequency focused on issues getting in the way of the right level of resilience
- Product/service level and resilience activity performance measurement
- Defined improvement-focused goals and objectives
- Automation to drive efficiency

Il y a quatre ans, j'ai mesuré le succès de sept manières importantes, et ces éléments à valeur ajoutée persistent aujourd'hui :

- Définition du périmètre par le biais de discussions avec les dirigeants
- Processus de continuité/résilience documentés et suivis par tous
- Des rôles clairs avec la participation des bonnes personnes
- Engagement à la bonne fréquence, axé sur les problèmes qui empêchent d'atteindre le niveau de résilience souhaité
- Mesure des performances au niveau des produits/services et des activités de résilience
- Définition d'objectifs axés sur l'amélioration
- Automatisation pour favoriser l'efficacité

Mais notre objectif pour 2026 est d'affiner notre définition de la capacité de résilience, en nous appuyant sur la disponibilité, la conception du contrôle des réponses et de la reprise, ainsi que la mise en œuvre et la mesure de l'efficacité opérationnelle.



But our 2026 focus is refining our definition of resilience capability, driven by availability, response and recovery control design and operating effectiveness implementation and measurement.

As such, Felder's business continuity and operating resilience program will measure success in a much-expanded manner:

- Faster executive decisions before and during disruption
- Fewer debates regarding what "good" resilience looks like
- Clear investment prioritization
- Reduced data and effort duplication across risk programs
- Greater confidence among key stakeholders
- A shared understanding of resilience as an operational capability

Perhaps most importantly, resilience is no longer "something Felder has".

It's something Felder **does** with controls built into our day-to-day operations. Ω

ABOUT THE AUTHOR

Brian Zawada has nearly thirty years of experience helping organizations manage the risk of disruption to the delivery of their most important products and services.

Brian began his career as an intelligence officer in the United States Air Force where had a key focus on "contingency planning". In the private sector, he has designed, implemented and led business continuity and operational resilience programs as an employee and consultant. Although Brian has served nearly all industries, his focus is on manufacturing, pharmaceutical/bio-technology and consumer products.

Brian has been awarded the Lifetime Achievement Award by The Business Continuity Institute and CIR Magazine. Brian has previously served as the President of the BCI US Chapter.

À ce titre, le programme de continuité des activités et de résilience opérationnelle de Felder mesurera le succès de manière beaucoup plus large :

- Décisions exécutives plus rapides avant et pendant les perturbations
- Moins de débats sur ce qu'est une « bonne » résilience
- Priorisation claire des investissements
- Réduction de la duplication des données et des efforts dans les programmes de gestion des risques
- Confiance accrue parmi les principales parties prenantes
- Une compréhension commune de la résilience en tant que capacité opérationnelle

Mais surtout, la résilience n'est plus « quelque chose que Felder possède ».

C'est quelque chose que Felder **met en œuvre** grâce à des contrôles intégrés à nos opérations quotidiennes. Ω

À PROPOS DE L'AUTEUR

Brian Zawada a près de trente ans d'expérience dans l'aide aux organisations pour la gestion des risques de perturbation dans la fourniture de leurs produits et services les plus importants.

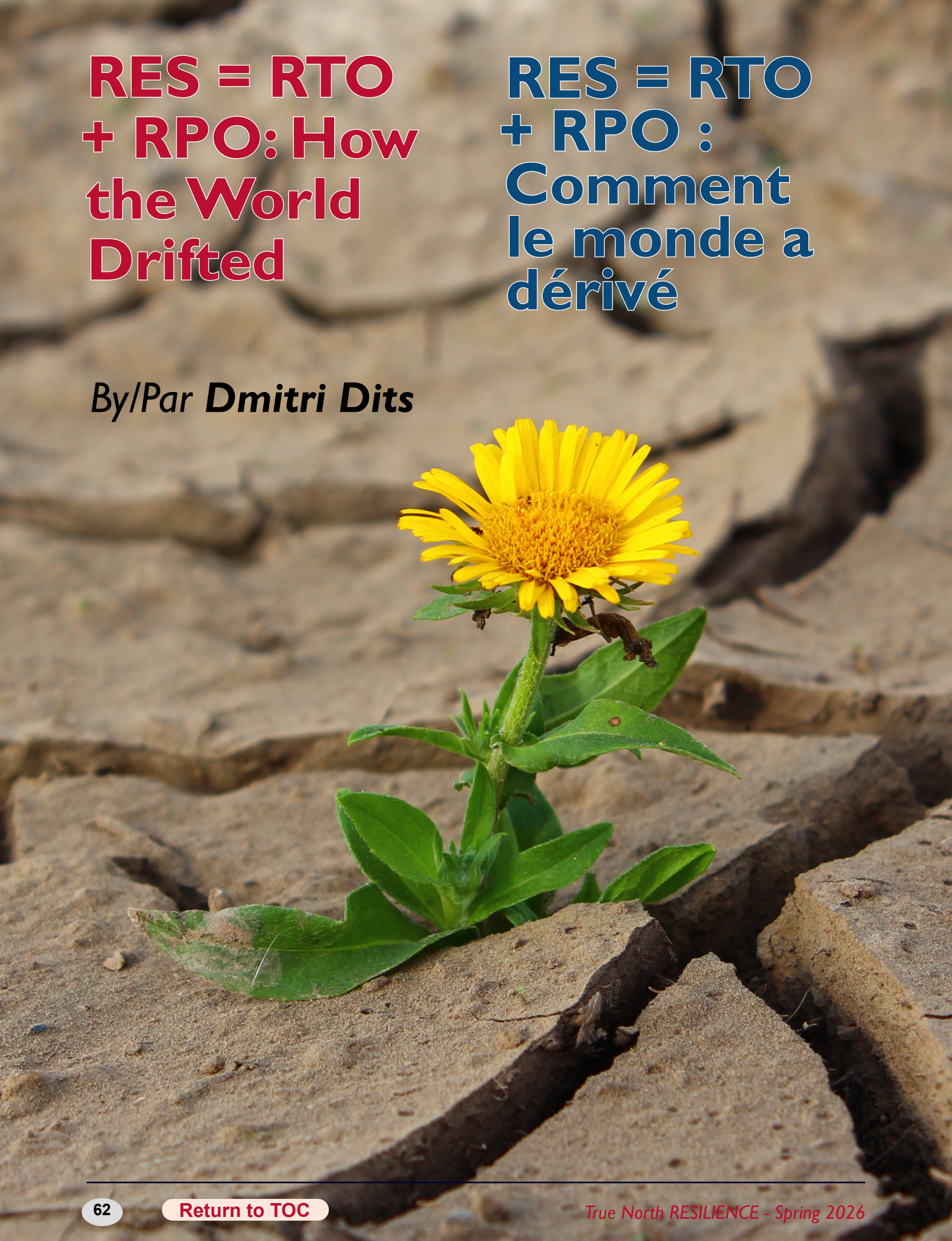
Brian a commencé sa carrière en tant qu'officier du renseignement dans l'armée de l'air américaine, où il s'est principalement concentré sur la « planification d'urgence ». Dans le secteur privé, il a conçu, mis en œuvre et dirigé des programmes de continuité des activités et de résilience opérationnelle en tant qu'employé et consultant. Bien que Brian ait travaillé dans presque tous les secteurs, il se concentre principalement sur l'industrie manufacturière, la pharmacie/biotechnologie et les produits de consommation.

Brian a reçu le Lifetime Achievement Award (prix d'excellence pour l'ensemble de sa carrière) décerné par le Business Continuity Institute et le magazine CIR. Brian a précédemment occupé le poste de président de la section américaine du BCI.

RES = RTO + RPO: How the World Drifted

RES = RTO + RPO : Comment le monde a dérivé

By/Par ***Dmitri Dits***



Did We Create a Monster Called "Resilience"?

How an Abstract Word Drifted Away from the Disciplines That Once Gave It Meaning

Over the past two decades, few words have gained as much prominence in emergency management, business continuity, and risk governance as resilience. It appears in strategy documents, funding proposals, board presentations, and regulatory guidance. Organizations aspire to it, leaders demand it, and consultants measure it. Yet when real disruptions occur, cyberattacks, infrastructure failures, natural disasters, the operational questions that determine survival remain stubbornly unchanged.

- ✓ How long can this function be unavailable?
- ✓ How much loss is acceptable?
- ✓ Who approved of those limits?

The uncomfortable truth is that resilience, as it is commonly used today, has drifted away from the concrete recovery disciplines that once defined it. In doing so, it has become less actionable, less testable, and less accountable.

The Post-9/11 Origin of the Drift

The modern rise of resilience can be traced to the aftermath of September 11, 2001. The attacks fundamentally altered how governments and organizations perceived disruption. Existing continuity concepts, contingency planning, redundancy, recovery timelines, were suddenly criticized as too narrow, too technical, and too siloed for a world shaped by terrorism, systemic risk, and cascading failure.

What was needed was a unifying word. One broad enough to span terrorism, natural disasters, infrastructure collapse, and social shock. One that could bridge agencies and

Avons-nous créé un monstre appelé « résilience » ?

Comment un mot abstrait s'est éloigné des disciplines qui lui donnaient autrefois tout son sens

Au cours des deux dernières décennies, peu de mots ont pris autant d'importance dans la gestion des urgences, la continuité des activités et la gouvernance des risques que celui de résilience. Il apparaît dans les documents stratégiques, les propositions de financement, les présentations aux conseils d'administration et les directives réglementaires. Les organisations y aspirent, les dirigeants l'exigent et les consultants la mesurent. Pourtant, lorsque de véritables perturbations surviennent, qu'il s'agisse de cyberattaques, de pannes d'infrastructures ou de catastrophes naturelles, les questions opérationnelles qui déterminent la survie restent obstinément inchangées.

- ✓ Combien de temps cette fonction peut-elle être indisponible ?
- ✓ Quel niveau de perte est acceptable ?
- ✓ Qui a approuvé ces limites ?

La vérité dérangeante est que la résilience, telle qu'elle est couramment utilisée aujourd'hui, s'est éloignée des disciplines concrètes de reprise qui la définissaient autrefois. Ce faisant, elle est devenue moins applicable, moins vérifiable et moins responsable.

L'origine de cette dérive après le 11 septembre

L'essor moderne de la résilience remonte aux conséquences du 11 septembre 2001. Les attentats ont fondamentalement modifié la façon dont les gouvernements et les organisations percevaient les perturbations. Les concepts existants de continuité, de planification d'urgence, de redondance et de délais de reprise ont soudainement été

sectors without forcing immediate agreement on limits, trade-offs, or definitions of failure.

Resilience quietly filled that gap.

From Descriptor to Doctrine

The shift became formalized in 2005 with the Hyogo Framework for Action, which elevated resilience from a descriptive quality to a global disaster risk reduction objective. From that moment forward, resilience was no longer merely an outcome – it became a policy goal.

This distinction matters. When resilience became the goal, continuity quietly became the method, often unnamed. Recovery mechanics were assumed rather than specified. The vocabulary changed faster than the work itself.

critiqués comme étant trop restrictifs, trop techniques et trop cloisonnés pour un monde marqué par le terrorisme, les risques systémiques et les défaillances en cascade.

Il fallait un mot fédérateur. Un mot suffisamment large pour englober le terrorisme, les catastrophes naturelles, l'effondrement des infrastructures et les chocs sociaux. Un mot qui puisse faire le lien entre les agences et les secteurs sans imposer un accord immédiat sur les limites, les compromis ou les définitions de l'échec.

La résilience a discrètement comblé ce vide.

Du descripteur à la doctrine

Ce changement a été officialisé en 2005 avec le Cadre d'action de Hyogo, qui a élevé la résilience du statut de qualité descriptive

By the late 2000s, governments, NGOs, and private organizations were launching resilience strategies, resilience initiatives, and resilience funding streams. Yet in practice, these programs still relied on the same tools' continuity professionals had always used: business impact analysis, essential function identification, recovery timelines, and acceptable loss thresholds. The work stayed concrete. The language became abstract.

Two Tracks, One Problem

By the 2010s, the separation was complete. Continuity standards such as NFPA 1600, ISO 22301, and continuity of operations doctrine continued to demand precision: Recovery Time Objectives, Recovery Point Objectives, and minimum acceptable functionality. Meanwhile, resilience evolved into a leadership virtue, a maturity label, an index, or a score.

Two parallel tracks emerged. Standards remained disciplined and executable. Language became aspirational and symbolic.

This is where the monster formed.

Today, resilience is often invoked repeatedly in meetings, used to justify decisions rather than measure them, and treated as an inherent quality rather than a demonstrable outcome. Yet when incidents are reviewed, evaluations still default to the same questions continuity disciplines have always asked: how long recovery took, how much was lost, and whether essential functions survived.

The math never changed. Only the word did.

The Unavoidable Equation

When stripped of abstraction, the operational definition of resilience is remarkably simple:

Resilience equals Recovery Time Objective plus Recovery Point Objective.

à celui d'objectif mondial de réduction des risques de catastrophe. À partir de ce moment, la résilience n'était plus seulement un résultat, elle est devenue un objectif politique.

Cette distinction est importante. Lorsque la résilience est devenue l'objectif, la continuité est discrètement devenue la méthode, souvent sans être nommée. Les mécanismes de reprise ont été supposés plutôt que spécifiés. Le vocabulaire a changé plus rapidement que le travail lui-même.

À la fin des années 2000, les gouvernements, les ONG et les organisations privées ont lancé des stratégies, des initiatives et des sources de financement en faveur de la résilience. Pourtant, dans la pratique, ces programmes d' s s'appuyaient toujours sur les mêmes outils que ceux que les professionnels de la continuité avaient toujours utilisés : analyse d'impact sur les activités, identification des fonctions essentielles, calendriers de reprise et seuils de perte acceptables. Le travail restait concret. Le langage est devenu abstrait.

Deux voies, un seul problème

Dans les années 2010, la séparation était totale. Les normes de continuité telles que NFPA 1600, ISO 22301 et la doctrine de la continuité des opérations continuaient d'exiger de la précision : objectifs de temps de reprise, objectifs de point de reprise et fonctionnalité minimale acceptable. Pendant ce temps, la résilience est devenue une vertu de leadership, un label de maturité, un indice ou un score.

Deux voies parallèles ont émergé. Les normes sont restées rigoureuses et applicables. Le langage est devenu ambitieux et symbolique.

C'est là que le monstre s'est formé.

Aujourd'hui, la résilience est souvent invoquée à plusieurs reprises lors des réunions, utilisée pour justifier des décisions plutôt que pour les mesurer, et traitée comme une qualité

Recovery Time defines how long a function can be unavailable.
Recovery Point defines the acceptable point of loss – data, service, or mission capability.

This equation is not theoretical. It is embedded across continuity standards, including NFPA 1600, ISO 22301, and continuity of operations doctrine.

Where Abstraction Becomes Dangerous

Resilience did not become problematic because it is wrong, but because it is often used without definition. When leaders say, "we need to be resilient," they frequently avoid answering the hard questions continuity disciplines were designed to force.

Without explicit recovery objectives, resilience becomes non-executable and non-testable. It cannot be audited. It cannot be enforced. In practice, abstraction does not inspire action, it replaces decisions.

inhérente plutôt que comme un résultat démontrable. Pourtant, lorsque les incidents sont examinés, les évaluations reviennent toujours aux mêmes questions que les disciplines de continuité ont toujours posées : combien de temps a pris la reprise, combien a été perdu et si les fonctions essentielles ont survécu.

Le calcul n'a jamais changé. Seul le mot a changé.

L'équation inévitable

Une fois dépouillée de son abstraction, la définition opérationnelle de la résilience est remarquablement simple :

La résilience est égale au temps de récupération cible plus le point de récupération cible.

Le temps de rétablissement définit la durée pendant laquelle une fonction peut être indisponible.
Le point de rétablissement définit le point de perte acceptable (données, service ou capacité opérationnelle).

Cette équation n'est pas théorique. Elle est intégrée dans les normes de continuité, notamment NFPA 1600, ISO 22301 et la doctrine de continuité des opérations.

Quand l'abstraction devient dangereuse

La résilience n'est pas devenue problématique parce qu'elle est erronée, mais parce qu'elle est souvent utilisée sans définition. Lorsque les dirigeants affirment « nous devons être résilients », ils évitent souvent de répondre aux questions difficiles que les disciplines de continuité ont été conçues pour imposer.

Sans objectifs de reprise explicites, la résilience devient inapplicable et non testable. Elle ne peut être auditée. Elle ne peut être appliquée. Dans la pratique, l'abstraction n'inspire pas l'action, elle remplace les décisions.

Restoring Meaning

Resilience itself is not the enemy. As a concept, it played a valuable role in bridging disciplines and sustaining attention during periods of uncertainty. The problem began when resilience stopped describing outcomes and started substituting for decisions.

When resilience is grounded in defined recovery time and acceptable loss, it regains its value. It becomes an honest summary of performance, not a promise or a posture.

Resilience works best when it is earned, after systems are tested and limits respected, not declared in advance. Ω

Redonner du sens

La résilience en soi n'est pas l'ennemie. En tant que concept, elle a joué un rôle précieux en reliant les disciplines et en maintenant l'attention pendant les périodes d'incertitude. Le problème a commencé lorsque la résilience a cessé de décrire les résultats et a commencé à se substituer aux décisions.

Lorsque la résilience est fondée sur un temps de rétablissement défini et une perte acceptable, elle retrouve sa valeur. Elle devient un résumé honnête de la performance, et non une promesse ou une posture.

La résilience fonctionne mieux lorsqu'elle est méritée, après que les systèmes ont été testés et les limites respectées, et non lorsqu'elle est déclarée à l'avance. Ω

ABOUT THE AUTHOR

***Dmitri Dits** serves as Chief Emergency Management Officer at the New York City Department of Buildings, leading crisis response and continuity planning. He oversees emergency management and continuity functions within a jurisdiction of more than 1.1 million buildings.*

Prior to immigrating to the United States, Dmitri completed technical education in Europe—in Ukraine—studying Environmental Engineering at Odessa Polytechnic University After relocating to the U.S., he earned a Bachelor of Science in Business Administration and Management from the City University of New York, Brooklyn College.

A Certified Business Continuity Professional (CBCP), Dmitri received the DRI International Award of Excellence (2020) and serves as a Commissioner Volunteer on the Certification Committee and awards review committee.

In parallel with his operational role, Dmitri conducts research on decision-making under uncertainty and developed the Unified Decision Construct (UDC). He works at the intersection of Emergency Management, Business Continuity, and Risk Management.

Dmitri resides on Long Island, New York, with his wife and two children.

À PROPOS DE L'AUTEUR

***Dmitri Dits** occupe le poste de directeur de la gestion des urgences au sein du département des bâtiments de la ville de New York, où il dirige les interventions en cas de crise et la planification de la continuité des activités. Il supervise la gestion des urgences et les fonctions de continuité au sein d'une juridiction comptant plus de 1,1 million de bâtiments. Avant d'immigrer aux États-Unis, Dmitri a suivi une formation technique en Europe, en Ukraine, où il a étudié l'ingénierie environnementale à l'université polytechnique d'Odessa. Après s'être installé aux États-Unis, il a obtenu une licence en administration et gestion des entreprises à la City University of New York, Brooklyn College. Certifié CBCP (Certified Business Continuity Professional), Dmitri a reçu le prix d'excellence DRI International (2020) et occupe les fonctions de commissaire bénévole au sein du comité de certification et du comité d'examen des récompenses. Parallèlement à son rôle opérationnel, Dmitri mène des recherches sur la prise de décision en situation d'incertitude et a développé le concept UDC (Unified Decision Construct). Il travaille à la croisée de la gestion des urgences, de la continuité des activités et de la gestion des risques.*
Dmitri réside à Long Island, New York, avec sa femme et ses deux enfants.

THE DEATH AND REBIRTH OF RISK MANAGEMENT

LA MORT ET LA RENAISSANCE DE LA GESTION DES RISQUES

By/Par **Patrick Ow**

Strategic Risk & Governance Professional & Coach | Turning Risk into a Catalyst for Strategy-Focused Decisions & Improved Performance | Simplifying Complexity for Better Results & Performance

Let me be uncomfortably direct: if you're still measuring your value as a risk professional by the comprehensiveness of your risk register, the elegance of your heat maps, or your compliance score, you're already on the path to professional irrelevance.

I don't say this to provoke. I say it because I've watched it happen. I've seen brilliant technical risk analysts sidelined during the moments that actually mattered. I've witnessed Chief Risk Officers excluded from the room where crisis decisions were made. The reality is that when the building is on fire, no one calls the person who updates the fire safety manual.

Professionnel et coach en gestion stratégique des risques et gouvernance | Transformer le risque en catalyseur pour des décisions axées sur la stratégie et l'amélioration des performances | Simplifier la complexité pour de meilleurs résultats et performances

Je vais être très direct : si vous continuez à mesurer votre valeur en tant que professionnel du risque à l'aune de l'exhaustivité de votre registre des risques, de l'élégance de vos cartes thermiques ou de votre score de conformité, vous êtes déjà sur la voie de l'irrélevance professionnelle.

Je ne dis pas cela pour provoquer. Je le dis parce que j'ai vu cela se produire. J'ai vu de brillants analystes techniques du risque mis à l'écart au moment où cela comptait vraiment. J'ai vu des directeurs de la gestion des risques exclus de la salle où se prenaient les décisions en cas de crise. La réalité est que lorsque le bâtiment est en feu, personne n'appelle la personne qui met à jour le manuel de sécurité incendie.

The uncomfortable truth? **The risk professionals are facing an existential crisis. And most practitioners don't even realise it.**

This isn't about whether risk management survives as a function – it will, because organisations need to navigate uncertainty, especially during a poly-crisis. This is about whether **you** survive as a risk professional, or whether you're replaced by someone from strategy, communications, data science, or operations who learned to speak the language of risk faster than you learned to speak the language of business.

The World Changed... Your Methodology Didn't.

Remember when crisis management meant preparing for "black swan" events – the rare, unpredictable disruptions that occurred every few years? That world is gone.

Welcome to polycrisis. The Russia-Ukraine war enters its fourth year. Gaza. Climate disasters occur quarterly, not generationally. CrowdStrike outages that cascade into global operational paralysis. AI disruption is happening at a pace that makes five-year plans absurd. DEI and ESG backlash are creating values-based flashpoints that were unimaginable a decade ago.

In January 2023, the World Economic Forum describes a shift toward "polycrisis," where multiple disruptions interact and compound. This reality changes **how trust is built and lost**. Organisations are judged less on perfection and more on **speed, honesty, and coherence under pressure**. Crisis management becomes a daily capability rather than a specialised function, and leadership credibility is forged in moments that were once considered edge cases.

Crisis is no longer the exception you plan around. **Crisis (and uncertainty) is the operating environment you navigate continuously.**

Yet our professional toolkit hasn't evolved. We're still:

- Conducting **quarterly risk reviews** in a world where the risk landscape changes weekly or monthly.
- Building **risk registers** that document what we already know, rather than detecting what's emerging.
- Creating **heat maps** that provide false precision about single risks while missing the cascading interactions that actually destroy organisations.

La vérité dérangeante ? **Les professionnels du risque sont confrontés à une crise existentielle. Et la plupart des praticiens ne s'en rendent même pas compte.**

Il ne s'agit pas de savoir si la gestion des risques survivra en tant que fonction – elle survivra, car les organisations doivent naviguer dans l'incertitude, en particulier pendant une polycrise. Il s'agit de savoir si **vous** survivrez en tant que professionnel du risque, ou si vous serez remplacé par quelqu'un issu de la stratégie, de la communication, de la science des données ou des opérations qui a appris à parler le langage du risque plus rapidement que vous n'avez appris à parler le langage des affaires.

Le monde a changé... Votre méthodologie, non.

Vous vous souvenez de l'époque où la gestion de crise consistait à se préparer à des événements « cygnes noirs », ces perturbations rares et imprévisibles qui se produisaient tous les quelques années ? Ce monde n'existe plus.

Bienvenue dans l'ère de la polycrise. La guerre entre la Russie et l'Ukraine entre dans sa quatrième année. Gaza. Les catastrophes climatiques se produisent tous les trimestres, et non plus tous les quarante ans. Les pannes de CrowdStrike entraînent une paralysie opérationnelle mondiale. Les bouleversements liés à l'IA se produisent à un rythme qui rend absurdes les plans quinquennaux. Les réactions négatives à l'égard de la DEI et de l'ESG créent des points chauds basés sur des valeurs qui étaient inimaginables il y a dix ans.

En janvier 2023, le Forum économique mondial décrit une évolution vers une « polycrise », où de multiples perturbations interagissent et se combinent. Cette réalité change **la façon dont la confiance se construit et se perd**. Les organisations sont moins jugées sur leur perfection que sur **leur rapidité, leur honnêteté et leur cohérence sous pression**. La gestion de crise devient une compétence quotidienne plutôt qu'une fonction spécialisée, et la crédibilité des dirigeants se forge dans des moments qui étaient autrefois considérés comme des cas extrêmes.

La crise n'est plus l'exception pour laquelle vous vous préparez. **La crise (et l'incertitude) est l'environnement opérationnel dans lequel vous évoluez en permanence.**

Pourtant, nos outils professionnels n'ont pas évolué. Nous continuons à :

- Designing **three lines of defence** that blur into confusion the moment a real crisis hits.
- Conduct overly linear **scenario planning** and single-hazard when a polycrisis means multiple simultaneous disruptions.
- Measuring **control effectiveness** when speed of response matters more than control perfection.

The brutal architecture of traditional risk management was built for stability, periodicity, and isolation of risks. The reality is that we now operate in volatility, continuity, and interdependence.

Our current risk methodology solves yesterday's problem, not proactively anticipates tomorrow's challenges.

The Four Horsemen of Risk Professional Obsolescence

Let me show you exactly how risk professionals become irrelevant:

Horseman 1: The Speed Gap

Your methodology requires deliberation. Crisis demands improvisation.

When a values-based controversy erupts on social media, stakeholders judge your organisation within **minutes**. Trust is gained or lost before you've scheduled the meeting to discuss scheduling a meeting about forming a working group to assess the situation.

The most important risk decisions are now made **before formal risk analysis is possible**. Let that sink in. Your primary professional skill – the traditional rigorous assessment – arrives too late to influence the outcome.

- Réalisons **des examens trimestriels des risques** dans un monde où le paysage des risques change chaque semaine ou chaque mois.
- Construisons **des registres de risques** qui documentent ce que nous savons déjà, plutôt que de détecter ce qui émerge.
- Créons **des cartes thermiques** qui fournissent une fausse précision sur des risques individuels tout en omettant les interactions en cascade qui détruisent réellement les organisations.
- Concevons **trois lignes de défense** qui s'estompent dans la confusion dès qu'une véritable crise survient.
- Nous menons **une planification de scénarios** trop linéaire et axée sur un seul risque, alors qu'une polycrise implique de multiples perturbations simultanées.
- Mesurer **l'efficacité des contrôles** alors que la rapidité de la réponse est plus importante que la perfection des contrôles.

L'architecture brutale de la gestion traditionnelle des risques a été conçue pour la stabilité, la périodicité et l'isolation des risques. La réalité est que nous opérons désormais dans un contexte de volatilité, de continuité et d'interdépendance.

Notre méthodologie actuelle en matière de risques résout les problèmes d'hier, mais n'anticipe pas de manière proactive les défis de demain.

Les quatre cavaliers de l'obsolescence des professionnels du risque

Laissez-moi vous montrer exactement comment les professionnels du risque deviennent inutiles :

Cavalier n° 1 : le décalage de vitesse

Votre méthodologie nécessite une réflexion approfondie. Les crises exigent de l'improvisation.

Lorsqu'une controverse fondée sur des valeurs éclate sur les réseaux sociaux, les parties prenantes jugent votre organisation en quelques **minutes**. La confiance est gagnée ou perdue avant même que vous ayez prévu une réunion pour discuter de la création d'un groupe de travail chargé d'évaluer la situation.

Communications teams, strategy teams, and operations teams have learned to move at crisis speed. If you can't, they'll make risk (or risky) decisions without you. And eventually, they'll stop inviting you entirely.

Horseman 2: The Integration Deficit

You're organised in silos. Crisis cascades across domains.

Your cyber team doesn't regularly talk to your supply chain team. Your operational risk specialists don't collaborate with your reputational risk advisors. Your compliance function operates independently of your strategic planning.

Then CrowdStrike happens: a technical cyber issue that instantly becomes an operational crisis that triggers reputational risk that creates strategic questions about resilience and vendor concentration.

Or your AI product produces biased outputs: a technical failure that ignites employee activism (HR crisis) that attracts regulatory scrutiny (compliance crisis) that generates customer backlash (commercial crisis) that raises board-level questions about leadership judgment (governance crisis).

Polycrisis means interconnected, compounding disruptions. If you can't see across domains quickly and help your leadership navigate interdependencies and impact, you're providing partial intelligence that's often more dangerous than no intelligence.

Horseman 3: The Values Blindspot

You were trained to assess operational and financial risks. The risks that now destroy organisations are moral and reputational.

When employees demand your organisation take a stand on Gaza, or ESG critics accuse you of "woke capitalism," or a return-to-office mandate triggers activism – these aren't risks you can control or transfer. These are identity and legitimacy risks that require quick judgment about organisational values, stakeholder expectations, and cultural dynamics.

Most risk professionals are spectacularly unprepared for this. You can quantify credit risk and cyber exposure. But can you help leadership navigate: "If we stay silent on this issue, employees will perceive us as complicit, but if we speak, we'll face political backlash in three key markets"?

Les décisions les plus importantes en matière de risques sont désormais prises **avant qu'une analyse formelle des risques ne soit possible**. Réfléchissez-y bien. Votre principale compétence professionnelle, l'évaluation rigoureuse traditionnelle, arrive trop tard pour influencer le résultat.

Les équipes de communication, de stratégie et d'exploitation ont appris à agir à la vitesse de la crise. Si vous n'en êtes pas capable, elles prendront des décisions risquées (ou risquées) sans vous. Et finalement, elles cesseront complètement de vous inviter.

Cavalier n° 2 : le déficit d'intégration

Vous êtes organisés en silos. La crise se propage à tous les domaines.

Votre équipe cyber ne communique pas régulièrement avec votre équipe chargée de la chaîne d'approvisionnement. Vos spécialistes des risques opérationnels ne collaborent pas avec vos conseillers en risques de réputation. Votre fonction de conformité fonctionne indépendamment de votre planification stratégique.

C'est alors que survient CrowdStrike : un problème technique lié à la cybersécurité qui se transforme instantanément en crise opérationnelle, déclenchant un risque de réputation qui soulève des questions stratégiques sur la résilience et la concentration des fournisseurs.

Ou bien votre produit d'IA produit des résultats biaisés : une défaillance technique qui déclenche l'activisme des employés (crise RH), qui attire l'attention des autorités de régulation (crise de conformité), qui génère une réaction négative des clients (crise commerciale), qui soulève des questions au niveau du conseil d'administration sur le jugement des dirigeants (crise de gouvernance).

Une polycrise signifie des perturbations interconnectées et cumulatives. Si vous ne pouvez pas avoir une vue d'ensemble rapide des différents domaines et aider vos dirigeants à gérer les interdépendances et les impacts, vous fournissez des informations partielles qui sont souvent plus dangereuses que l'absence d'informations.

Cavalier n° 3 : l'angle mort des valeurs

Vous avez été formé pour évaluer les risques opérationnels et financiers. Les risques qui détruisent aujourd'hui les organisations sont d'ordre moral et réputationnel.

Lorsque les employés exigent que votre organisation prenne position sur Gaza, que les détracteurs ➤

Every major organisational decision is now a reputational or trust act. If you're not equipped to assess values-based risks with the same rigour you assess financial risks, you're missing the threats most likely to destroy stakeholder trust.

Horseman 4: The Credibility Chasm

You speak the language of probability and controls. Leadership needs strategic intelligence and judgment.

Walk into a board meeting and present your beautifully formatted risk register with likelihood scores and impact ratings. Watch eyes glaze over.

You've provided data, not practical insights. Documentation, not foresight. Process, not intelligence.

Now watch what happens when the strategy consultant walks in and says: "Three trends are converging that will fundamentally reshape this industry in 18 months. Here's how you position for advantage while competitors freeze in uncertainty." That person just became more valuable than you.

Risk professionals are perceived as compliance 'bureaucrats', not strategic partners. Until you change that perception through demonstrated value, you'll never get the seat at the table where decisions are actually shaped.

The Brutal Math of Professional Displacement

Here's what's happening right now, whether you see it or not:

Scenario A: Your organisation faces a major crisis. The CEO convenes the response team: Operations, Communications, Legal, HR, Strategy. You, the risk professional, find out about it afterwards. You are asked to document what happened for the risk register.

Scenario B: Your company is considering entering a challenging new market. Strategy develops the business case. Finance models the returns. Operations assesses feasibility. You're asked to "review for risks" after the decision is essentially made. You're a checkpoint, not a partner.

Scenario C: A values-based controversy erupts. Communications and HR are managing the response in real-time. You hear about it when someone asks you to update the reputational risk assessment for the next quarterly review.

de l'ESG vous accusent de « capitalisme woke » ou que l'obligation de retour au bureau déclenche un activisme, ce ne sont pas des risques que vous pouvez contrôler ou transférer. Il s'agit de risques liés à l'identité et à la légitimité qui nécessitent un jugement rapide sur les valeurs organisationnelles, les attentes des parties prenantes et la dynamique culturelle.

La plupart des professionnels du risque sont totalement démunis face à cela. Vous pouvez quantifier le risque de crédit et l'exposition cyber. Mais pouvez-vous aider la direction à naviguer entre deux feux : « Si nous restons silencieux sur cette question, les employés nous percevront comme complices, mais si nous nous exprimons, nous ferons face à un retour de bâton politique sur trois marchés clés » ?

Chaque décision organisationnelle majeure est désormais un acte qui engage la réputation ou la confiance. Si vous n'êtes pas en mesure d'évaluer les risques liés aux valeurs avec la même rigueur que les risques financiers, vous passez à côté des menaces les plus susceptibles de détruire la confiance des parties prenantes.

Cavalier n° 4 : le fossé de la crédibilité

Vous parlez le langage des probabilités et des contrôles. Le leadership nécessite une intelligence stratégique et du jugement.

Entrez dans une réunion du conseil d'administration et présentez votre registre des risques magnifiquement formaté, avec des scores de probabilité et des notes d'impact. Regardez les yeux se voiler.

Vous avez fourni des données, pas des informations pratiques. De la documentation, pas de la prévoyance. Des processus, pas de l'intelligence.

Observez maintenant ce qui se passe lorsque le consultant en stratégie entre et déclare : « Trois tendances convergent et vont profondément remodeler ce secteur dans les 18 prochains mois. Voici comment vous positionner pour en tirer parti pendant que vos concurrents restent paralysés par l'incertitude. » Cette personne vient de devenir plus précieuse que vous.

Les professionnels du risque sont perçus comme des « bureaucrates » chargés de la conformité, et non comme des partenaires stratégiques. Tant que vous n'aurez pas changé cette perception en démontrant votre valeur, vous n'aurez jamais votre place à la table où se prennent réellement les décisions.

In each scenario, you're peripheral. Reactive. After the fact. **You're becoming the organisational historian, not the strategic architect.**

And here's the terrifying part: you might not even notice it happening. You're still busy. You have meetings. You produce reports. Your KPIs might even look good – 100% of risks documented, 95% of controls tested, zero audit findings.

But you're optimising for metrics that no longer matter. You're excelling at a job that's ceasing to be relevant.

The Three Radical Shifts That Determine Professional Survival

If you want to avoid obsolescence, you must make three fundamental transformations in how you conceive of your role:

Shift 1: From Gatekeeper to Value Creator

Traditional identity: You're the person who says "no" to protect the organisation.

Required identity: You're the person who enables calculated speed and identifies competitive advantage in volatility, or during a crisis.

Why it matters: In a polycrisis environment where every competitor faces the same turbulence, the differentiator is who navigates uncertainty most effectively and in the shortest possible time. When your competitor's supply chain collapses, having the most resilient alternative is a market-share opportunity. When regulatory uncertainty paralyses the industry, moving decisively while others freeze creates a positioning advantage.

Practical transformation: Stop framing your work as "here's what we can't do." Start framing it

La mathématique brutale du déplacement professionnel

Voici ce qui se passe actuellement, que vous le voyiez ou non :

Scénario A : votre organisation est confrontée à une crise majeure. Le PDG convoque l'équipe d'intervention : opérations, communication, juridique, RH, stratégie. Vous, le professionnel du risque, l'apprenez après coup. On vous demande de documenter ce qui s'est passé pour le registre des risques.

Scénario B : votre entreprise envisage de se lancer sur un nouveau marché difficile. La stratégie élabore l'analyse de rentabilité. Les finances modélisent les rendements. Les opérations évaluent la faisabilité. On vous demande d'« examiner les risques » après que la décision a été prise. Vous êtes un point de contrôle, pas un partenaire.

Scénario C : une controverse liée aux valeurs éclate. Les services de communication et des ressources humaines gèrent la réponse en temps réel. Vous en entendez parler lorsque quelqu'un vous demande de mettre à jour l'évaluation des risques pour la réputation en vue de la prochaine revue trimestrielle.

Dans chaque scénario, vous êtes en périphérie. Réactif. Après coup. **Vous devenez l'historien de l'organisation, et non son architecte stratégique.**

Et voici le plus effrayant : vous ne vous en rendez peut-être même pas compte. Vous êtes toujours occupé. Vous avez des réunions. Vous produisez des rapports. Vos indicateurs clés de performance peuvent même sembler bons : 100 % des risques documentés, 95 % des contrôles testés, zéro constat d'audit.

Mais vous optimisez des indicateurs qui n'ont plus d'importance. Vous excellez dans un travail qui n'est plus pertinent.

Les trois changements radicaux qui déterminent la survie professionnelle

Si vous voulez éviter l'obsolescence, vous devez opérer trois transformations fondamentales dans la façon dont vous concevez votre rôle :

Changement n° 1 : passer de gardien à créateur de valeur

as "**here's how we move faster than competitors while managing exposure intelligently**."

In your next strategic planning session, don't just present risks to mitigate. Present **opportunities that emerge from volatility** and how your risk capabilities enable capturing them faster than competitors who lack your infrastructure.

Example: "Our supply chain resilience investments allow us to guarantee delivery when competitors can't. In the next geopolitical disruption, we should plan aggressive customer acquisition targeting their vulnerable accounts. I can have response playbooks ready in 30 days."

That's a risk professional creating value, not preventing action.

Shift 2: From Second Line to Strategic Partner

Traditional position: You're part of the "three lines of defence" – independent assurance reviewing what others do.

Required position: You're in the room when strategy is being shaped, providing intelligence that influences decisions before they're made.

Why it matters: The Chief Risk Officer role is evolving to parallel the CFO. Just as the CFO translates the financial implications of strategy, the CRO must translate the volatility implications and interdependencies. This isn't risk reporting. This is strategic intelligence.

Leadership credibility is now forged in crisis moments that were once considered edge cases. The executive who understands the interdependence of DEI, ESG, cyber, geopolitical, and operational risks, which helps the organisation maintain coherence across them, becomes indispensable.

Practical transformation: Map which strategic decisions in your organisation last quarter were made without risk input until after the fact. For each one, write a one-page brief showing what risk intelligence would have added to decision quality.

Share this with your executive sponsor or CEO with this message: "I want to demonstrate the value of earlier risk integration. Here's what you would have known if we'd been involved when these decisions were being shaped, not after."

You're making the case for a seat at the strategy table, not the compliance table.

Identité traditionnelle : vous êtes la personne qui dit « non » pour protéger l'organisation.

Identité requise : vous êtes la personne qui permet une vitesse calculée et identifie l'avantage concurrentiel dans un contexte de volatilité ou de crise.

Pourquoi est-ce important ? Dans un environnement de crises multiples où tous les concurrents sont confrontés aux mêmes turbulences, ce qui fait la différence, c'est la capacité à naviguer dans l'incertitude de la manière la plus efficace et la plus rapide possible. Lorsque la chaîne d'approvisionnement de vos concurrents s'effondre, disposer de l'alternative la plus résiliente vous offre une opportunité de gagner des parts de marché. Lorsque l'incertitude réglementaire paralyse le secteur, agir de manière décisive alors que les autres restent figés vous confère un avantage en termes de positionnement.

Transformation pratique : cessez de présenter votre travail comme « voici ce que nous ne pouvons pas faire ». Commencez à le présenter comme « **voici comment nous pouvons aller plus vite que nos concurrents tout en gérant intelligemment notre exposition** ».

Lors de votre prochaine session de planification stratégique, ne vous contentez pas de présenter les risques à atténuer. Présentez **les opportunités qui découlent de la volatilité** et expliquez comment vos capacités en matière de gestion des risques vous permettent de les saisir plus rapidement que vos concurrents qui ne disposent pas de votre infrastructure.

Exemple : « Nos investissements dans la résilience de notre chaîne d'approvisionnement nous permettent de garantir la livraison alors que nos concurrents ne le peuvent pas. Lors de la prochaine perturbation géopolitique, nous devrions planifier une acquisition agressive de clients en ciblant leurs comptes vulnérables. Je peux préparer des plans d'action dans les 30 jours. »

C'est ainsi qu'un professionnel du risque crée de la valeur, sans empêcher l'action.

Changement n° 2 : passer de la deuxième ligne à un partenaire stratégique

Position traditionnelle : vous faites partie des « trois lignes de défense » – une assurance indépendante qui examine ce que font les autres.

Position requise : vous êtes présent lorsque la stratégie est élaborée, fournissant des informa-

Example: When your company is evaluating a major technology investment, you're in initial discussions providing intelligence like: "This vendor has concentration risk – 30% of our industry uses them. A single outage creates a coordinated vulnerability. I recommend we design for redundancy, which adds 15% cost but eliminates correlated risk. Here's the competitive advantage if we're the only major player still operating during their next outage."

That's a strategic partnership, not control testing.

Shift 3: From Spreadsheet Analyst to Bilingual Strategist

Traditional skillset: Quantitative analysis, control design, compliance expertise.

Required skillset: Data-driven pattern recognition **AND** sophisticated human judgment (and intuition) for navigating values-based crises.

Why it matters: The future risk professional must be bilingual—capable of leveraging AI and advanced analytics for predictive intelligence while exercising nuanced judgment about culture, values, stakeholder expectations, and organisational identity.

The technical side: Static spreadsheets are being displaced by:

- AI-powered pattern recognition that detects weak signals before they cascade.
- Natural language processing analyses sentiment across millions of social media posts.
- Predictive models identifying risk interdependencies.
- Agentic AI systems that take autonomous defensive actions within pre-approved parameters.

If you're not developing these capabilities, someone from data science will. And they'll take your job while adding predictive intelligence you can't match.

The human side: When DEI controversy erupts, when geopolitical violence demands a quick organisational response, when employee activism challenges leadership, these require judgment that no algorithm provides. Understanding stakeholder psychology, cultural nuance, value tensions, and organisational identity becomes as critical as technical risk assessment.

tions qui influencent les décisions avant qu'elles ne soient prises.

Pourquoi est-ce important ? Le rôle du directeur des risques évolue pour devenir parallèle à celui du directeur financier. Tout comme le directeur financier traduit les implications financières de la stratégie, le directeur des risques doit traduire les implications de la volatilité et les interdépendances. Il ne s'agit pas de rapports sur les risques, mais d'informations stratégiques.

La crédibilité du leadership se forge désormais dans des moments de crise qui étaient autrefois considérés comme des cas extrêmes. Le cadre qui comprend l'interdépendance des risques DEI, ESG, cybernétiques, géopolitiques et opérationnels, et qui aide l'organisation à maintenir une cohérence entre eux, devient indispensable.

Transformation pratique : identifiez les décisions stratégiques prises au cours du dernier trimestre dans votre organisation sans prise en compte des risques avant coup. Pour chacune d'entre elles, rédigez un résumé d'une page montrant en quoi l'intelligence des risques aurait amélioré la qualité de la décision.

Partagez ce document avec votre sponsor exécutif ou votre PDG en lui transmettant le message suivant : « Je souhaite démontrer la valeur d'une intégration précoce des risques. Voici ce que vous auriez su si nous avions été impliqués lors de l'élaboration de ces décisions, et non après coup. »

Vous plaidez en faveur d'une place à la table stratégique, et non à la table de la conformité.

Exemple : lorsque votre entreprise évalue un investissement technologique majeur, vous participez aux discussions initiales en fournissant des informations telles que : « Ce fournisseur présente un risque de concentration : 30 % de notre secteur l'utilise. Une seule panne crée une vulnérabilité coordonnée. Je recommande que nous concevions un système redondant, ce qui ajoute 15 % de coût mais élimine le risque corrélé. Voici l'avantage concurrentiel dont nous bénéficierions si nous étions le seul acteur majeur encore opérationnel lors de leur prochaine panne. »

Il s'agit d'un partenariat stratégique, et non d'un test de contrôle.

Changement n° 3 : de l'analyste de feuilles de calcul au stratège bilingue

Compétences traditionnelles : analyse quantitative, conception de contrôles, expertise en matière de conformité.

Practical transformation: Audit your skillset honestly. Score yourself 1-10 on:

- Advanced data analytics and visualisation
- AI and machine learning applications
- Predictive modeling and pattern recognition
- Strategic business acumen and industry dynamics
- Communication and storytelling for executive audiences
- Values-based decision frameworks and ethical reasoning
- Stakeholder psychology and cultural intelligence
- Crisis communication and narrative development

Where are you below 6? Those are professional development imperatives, not nice-to-haves.

Example: You deploy AI monitoring that detects emerging supply chain stress in a region 48 hours before it becomes a crisis (technical capability).

« GESTION DES RISQUES »

Compétences requises : reconnaissance de modèles basée sur les données **ET** jugement humain sophistiqué (et intuition) pour naviguer dans les crises liées aux valeurs.

Pourquoi est-ce important ? Le futur professionnel du risque doit être bilingue, capable d'exploiter l'IA et les analyses avancées pour obtenir des informations prédictives tout en exerçant un jugement nuancé sur la culture, les valeurs, les attentes des parties prenantes et l'identité organisationnelle.

L'aspect technique : les feuilles de calcul statiques sont remplacées par :

- La reconnaissance de modèles alimentée par l'IA qui détecte les signaux faibles avant qu'ils ne se propagent.
- Le traitement du langage naturel analyse les sentiments exprimés dans des millions de publications sur les réseaux sociaux.
- Modèles prédictifs identifiant les interdépendances en matière de risques.
- Les systèmes d'IA agentique prennent des mesures défensives autonomes dans le cadre de paramètres préapprouvés.

Si vous ne développez pas ces capacités, quelqu'un issu du domaine de la science des données le fera. Et cette personne prendra votre place tout en apportant une intelligence prédictive que vous ne pouvez égaler.

Le côté humain : lorsque des controverses liées à la diversité, l'équité et l'inclusion éclatent, lorsque la violence géopolitique exige une réponse rapide de la part de l'organisation, lorsque l'activisme des employés remet en question le leadership, cela nécessite un jugement qu'aucun algorithme ne peut fournir. Comprendre la psychologie des parties prenantes, les nuances culturelles, les tensions entre les valeurs et l'identité organisationnelle devient aussi essentiel que l'évaluation technique des risques.

Transformation pratique : évaluez honnêtement vos compétences. Notez-vous sur une échelle de 1 à 10 pour :

- Analyse et visualisation avancées des données
- Applications de l'IA et de l'apprentissage automatique
- Modélisation prédictive et reconnaissance de formes

You then help leadership navigate: "If we exit this supplier relationship, it impacts 200 local jobs in a community where we've positioned as a partner. How do we balance operational needs with social license?" (human judgment).

That's the bilingual capability that makes you irreplaceable.

The Strategic Risk Resilience Framework: Your Professional Survival Architecture

Let me give you something concrete. It's a framework I've developed specifically for risk professionals navigating this transformation. I call it the **Strategic Risk Resilience (SRR) Framework**, and it's built on six integrated pillars:

1. SENSING (Risk Intelligence & Foresight) – Move from periodic risk identification to continuous predictive intelligence. Deploy AI-powered monitoring that detects patterns before a crisis. Map interdependencies so you see cascade effects leadership misses.

2. STRUCTURE (Governance & Decision Architecture) – Design decision infrastructure that enables fast, coherent action. Establish crisis cells with clear authorities. Create "glocal" governance – global principles with local adaptation. Pre-authorise responses so you're not starting from zero during a crisis.

3. STANCE (Values Alignment & Strategic Position) – Stress-test organisational values against realistic dilemmas. Map stakeholder expectations and inherent tensions. Build authenticity by ensuring capabilities support commitments.

4. SCENARIOS (Adaptive Planning & Stress Testing) – Conduct compound stress tests where multiple crises hit simultaneously. Build scenario libraries that reveal interdependencies. Use business experiments to test at small scale before full commitment. Plan for competitive advantage capture during volatility.

5. SPEED (Response Capability & Execution) – Enable response in hours, not days. Pre-stage resources, pre-draft holding statements, and pre-identify experts. Build distributed risk literacy so decisions happen at the edge. Coordinate across functions without gridlock.

6. SYNTHESIS (Learning & Continuous Improvement) – Capture learning from every event

- Sens stratégique des affaires et dynamique du secteur
- Communication et narration pour un public de cadres supérieurs
- Cadres décisionnels fondés sur des valeurs et raisonnement éthique
- Psychologie des parties prenantes et intelligence culturelle
- Communication de crise et développement narratif

Où vous situez-vous en dessous de 6 ? Il s'agit là d'impératifs de développement professionnel, et non de simples atouts.

Exemple : vous déployez un système de surveillance par IA qui détecte les tensions émergentes dans la chaîne d'approvisionnement d'une région 48 heures avant qu'elles ne se transforment en crise (capacité technique). Vous aidez ensuite la direction à prendre les bonnes décisions : « Si nous mettons fin à cette relation avec le fournisseur, cela aura un impact sur 200 emplois locaux dans une communauté où nous nous sommes positionnés comme partenaire. Comment trouver un équilibre entre les besoins opérationnels et la licence sociale ? » (jugement humain).

C'est cette capacité bilingue qui vous rend irremplaçable.

Le cadre stratégique de résilience aux risques : votre architecture de survie professionnelle

Permettez-moi de vous donner un exemple concret. Il s'agit d'un cadre que j'ai développé spécialement pour les professionnels du risque qui naviguent dans cette transformation. Je l'appelle le **cadre de résilience stratégique face aux risques (SRR)** et il repose sur six piliers intégrés :

1. PERCEPTION (intelligence des risques et prévoyance) – Passez de l'identification périodique des risques à une intelligence prédictive continue. Déployez une surveillance alimentée par l'IA qui détecte les schémas avant une crise. Cartographiez les interdépendances afin de voir les effets en cascade que les dirigeants ne voient pas.

2. STRUCTURE (gouvernance et architecture décisionnelle) – Concevez une infrastructure décisionnelle qui permet une action rapide et cohérente. Mettez en place des cellules de crise

through structured after-action reviews. Track resilience metrics – speed of escalation, decision coherence, trust recovery time, adaptive capacity. Build a no-blame culture that rewards transparency. Evolve the framework continuously.

Why this framework matters for your career: It positions you as an architect of organisational resilience, not a documenter of risks. It gives you a structured approach to demonstrating value at every level. It aligns with ISO 31000, so you maintain professional rigour while being practically actionable.

Most importantly, it reframes the conversation from "What risks should we avoid?" to "**How do we navigate continuous uncertainty with speed, coherence, and competitive advantage?**"

That reframing is how you move from a cost centre to a strategic differentiator.

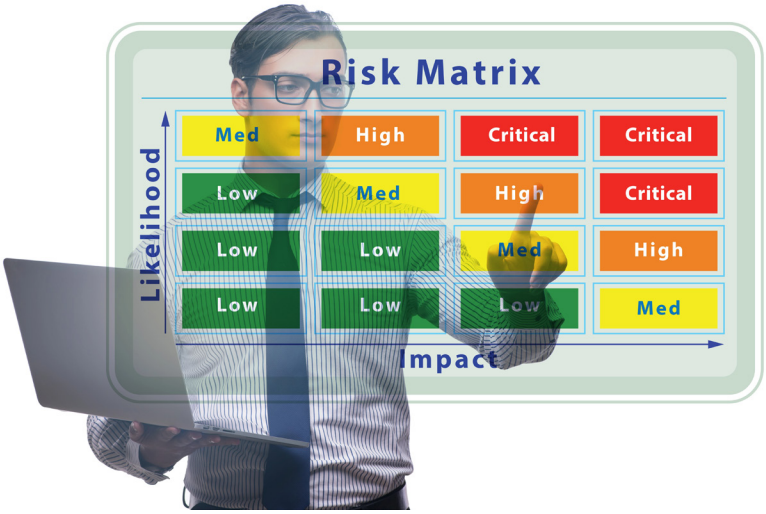
How do we navigate continuous uncertainty with speed, coherence, and competitive advantage?

What This Transformation Looks Like in Practice

Let me show you the difference between the old risk professional and the one who survives:

Old Model Risk Professional

Monthly risk committee meeting: "Here's our updated risk register. We've identified 47 risks across 12 categories. Seventeen are rated high. We recommend enhancing controls in these areas. Questions?"



dotées d'autorités claires. Créez une gouvernance « glocale » – des principes globaux adaptés au contexte local. Préautorisez les réponses afin de ne pas partir de zéro en cas de crise.

3. POSITION (alignement des valeurs et position stratégique) – Testez les valeurs organisationnelles face à des dilemmes réalistes. Cartographiez les attentes des parties prenantes et les tensions inhérentes. Renforcez l'authenticité en vous assurant que les capacités soutiennent les engagements.

4. SCÉNARIOS (planification adaptative et tests de résistance) – Réalisez des tests de résistance composites dans lesquels plusieurs crises surviennent simultanément. Créez des bibliothèques de scénarios qui révèlent les interdépendances. Utilisez des expériences commerciales d' s pour tester à petite échelle avant de vous engager pleinement. Prévoyez de tirer parti de l'avantage concurrentiel pendant la période de volatilité.

5. RAPIDITÉ (capacité de réponse et exécution) – Permettre une réponse en quelques heures, et non en quelques jours. Préparer les ressources, rédiger à l'avance des déclarations et identifier à l'avance les experts. Développer une culture du risque distribuée afin que les décisions soient prises au plus près du terrain. Coordonner les différentes fonctions sans blocage.

6. SYNTHÈSE (apprentissage et amélioration continue) – Tirez les leçons de chaque événement grâce à des analyses structurées après action. Suivez les indicateurs de résilience : rapidité de l'escalade, cohérence des décisions, temps de rétablissement de la confiance, capacité d'adaptation. Instaurez une culture sans reproches qui récompense la transparence. Faites évoluer le cadre en permanence.

Pourquoi ce cadre est-il important pour votre carrière ? Il vous positionne comme un architecte de la résilience organisationnelle, et non comme un simple documentateur des risques. Il vous offre une approche structurée pour démontrer votre valeur à tous les niveaux. Il est conforme à la norme ISO 31000, ce qui vous permet de conserver votre rigueur professionnelle tout en étant pragmatique.

Plus important encore, il recentre la conversation de « Quels risques devons-nous éviter ? » à « **Comment naviguer dans l'incertitude permanente avec rapidité, cohérence et avantage concurrentiel ?** ».

C'est grâce à ce recentrage que vous passez d'un centre de coûts à un facteur de différenciation stratégique.

Crisis response: Finds out about a major reputational crisis 12 hours after it begins. Asked to "assess the risk exposure" while Communications and HR are already managing the response. Produces a risk assessment three days later that documents what everyone already knows.

Strategic planning: Receives draft strategy from business units. Conducts "risk review" that identifies why various initiatives might fail. Seen as an obstacle to strategy, not a contributor to it.

Board interaction: Presents quarterly risk dashboard with heat maps and trend charts. Board members check phones. No questions asked. Five minutes allocated.

Career trajectory: Laterally stuck. Seen as competent but not strategic. Not invited to succession planning conversations. Eventually displaced by a younger professional from strategy consulting who "also understands risk."

Transformed Risk Professional

Weekly risk pulse session: "Three weak signals detected this week: Social media sentiment shifting on competitor's labour practices – potential industry contagion. Geopolitical tensions are rising in Region X, where we have tier-two supplier concentration. DEI sentiment among employees is declining – an early indicator of potential activism. Here's what I'm monitoring and at what threshold I recommend action."

Crisis response: Risk professional is in the crisis cell because they're positioned as a strategic intelligence provider. Provides real-time interdependency analysis: "If we take Position A, here's the cascade to employee sentiment, regulatory exposure, and market access. If we take Position B, here's the different cascade. Here's the stakeholder tension either way.

Comment naviguer dans l'incertitude permanente avec rapidité, cohérence et avantage concurrentiel ?

À quoi ressemble cette transformation dans la pratique ?

Permettez-moi de vous montrer la différence entre l'ancien professionnel du risque et celui qui survit :

Ancien modèle de professionnel du risque

Réunion mensuelle du comité des risques : « Voici notre registre des risques mis à jour. Nous avons identifié 47 risques répartis en 12 catégories. Dix-sept d'entre eux sont classés comme élevés. Nous recommandons de renforcer les contrôles dans ces domaines. Des questions ? »

Réponse à la crise : découvre une crise majeure affectant la réputation de l'entreprise 12 heures après son déclenchement. On lui demande d'« évaluer l'exposition au risque » alors que les services de communication et des ressources humaines gèrent déjà la réponse. Il produit trois jours plus tard une évaluation des risques qui documente ce que tout le monde sait déjà.

Planification stratégique : reçoit le projet de stratégie des unités opérationnelles. Procède à un « examen des risques » qui identifie les raisons pour lesquelles diverses initiatives pourraient échouer. Considéré comme un obstacle à la stratégie, et non comme un contributeur à celle-ci.

Interaction avec le conseil d'administration : présente un tableau de bord trimestriel des risques avec des cartes thermiques et des graphiques de tendance. Les membres du conseil d'administration consultent leurs téléphones. Aucune question n'est posée. Cinq minutes sont allouées.

Trajectoire de carrière : bloqué latéralement. Considéré comme compétent mais pas stratégique. N'est pas invité aux discussions sur la planification de la relève. Finit par être remplacé par un jeune professionnel issu du conseil en stratégie qui « comprend également les risques ».

Professionnel du risque transformé

Session hebdomadaire sur les risques :
« Trois signaux faibles ont été détectés cette semaine : le sentiment sur les réseaux sociaux évolue concernant les pratiques de travail des concurrents, ce qui pourrait avoir un effet contagieux sur le secteur. Les tensions géopolitiques s nt d'augmenter dans la région X, où se concentrent nos fournisseurs de deuxième niveau. Le sentiment des employés à l'égard de la diversité, de l'équité et de l'inclusion est en baisse, ce qui est un indicateur précoce d'un activisme potentiel. Voici ce que je surveille et le seuil à partir duquel je recommande d'agir. »

Réponse à la crise : le professionnel du risque fait partie de la cellule de crise, car il est considéré comme un fournisseur d'informations stratégiques. Il fournit une analyse en temps réel des interdépendances : « Si nous adoptons la position A, voici

And here's how this connects to our stated values from the stress test we did last quarter."

Strategic planning: Embedded in strategy development from the beginning. Contributes: "This market entry opportunity is actually enhanced by current volatility because competitors with weaker supply chains can't commit. We should accelerate, not delay. Here's the exposure we're taking and how we'll manage it. This is how we turn their risk into our advantage."

Board interaction: Presents strategic foresight briefing: "Three macro trends are converging that reshape our risk landscape: [explains implications]. This creates these vulnerabilities but also these opportunities. Competitors X and Y are particularly exposed here—we should consider these strategic moves. Questions typically include: 'How fast can we move on that opportunity?' and 'What do you need from us to strengthen that capability?'"

Career trajectory: Promoted to an expanded role. Invited into succession conversations. Recognised as a strategic partner to the CEO. Recruited by other organisations at a significant premium. Asked to speak at industry conferences on "risk as competitive advantage."

The difference? Not intelligence. Not work ethic. Not technical competence. **Strategic positioning and demonstrated value.**

The New Archetype: Risk as Leadership Function

In a permacrisis world, risk management does not disappear. It becomes indistinguishable from leadership itself.

The future risk professional is not a compliance expert, control designer, or policy custodian. They are:

- A **systems thinker** who sees patterns and interdependencies that others miss.
- A **trust strategist** who understands how legitimacy is built and lost.
- A **crisis translator** who moves seamlessly between technical depth and strategic clarity.
- A **value creator** who identifies how volatility creates competitive advantage.
- A **facilitator of principled action** who enables fast decisions when certainty is impossible.

les répercussions sur le sentiment des employés, l'exposition réglementaire et l'accès au marché. Si nous adoptons la position B, voici les répercussions différentes. Voici les tensions entre les parties prenantes dans les deux cas. Et voici comment cela se rapporte à nos valeurs déclarées lors du test de résistance que nous avons effectué au trimestre dernier.»

Planification stratégique : intégré dès le début dans l'élaboration de la stratégie. Contribution : « Cette opportunité d'entrée sur le marché est en fait renforcée par la volatilité actuelle, car les concurrents dont les chaînes d'approvisionnement sont plus faibles ne peuvent pas s'engager. Nous devons accélérer, et non retarder. Voici l'exposition que nous prenons et la manière dont nous allons la gérer. Voici comment nous transformons leur risque en avantage pour nous. »

Interaction avec le conseil d'administration : Présente un briefing sur les perspectives stratégiques : « Trois macro-tendances convergent et redessinent notre paysage de risques : [explique les implications]. Cela crée des vulnérabilités, mais aussi des opportunités. Les concurrents X et Y sont particulièrement exposés ici — nous devrions envisager ces mesures stratégiques. Les questions posées sont généralement les suivantes : « À quelle vitesse pouvons-nous saisir cette opportunité ? » et « De quoi avez-vous besoin de notre part pour renforcer cette capacité ? »

Parcours professionnel : Promotion à un poste plus important. Invitation à participer aux discussions sur la succession. Reconnu comme un partenaire stratégique du PDG. Recruté par d'autres organisations à un salaire nettement supérieur. Invité à prendre la parole lors de conférences sectorielles sur le thème « Le risque comme avantage concurrentiel ».

La différence ? Ce n'est pas l'intelligence. Ce n'est pas l'éthique de travail. Ce n'est pas la compétence technique. C'est **le positionnement stratégique et la valeur démontrée.**

Le nouvel archétype : le risque comme fonction de leadership

Dans un monde en crise permanente, la gestion des risques ne disparaît pas. Elle devient indissociable du leadership lui-même.

Le futur professionnel du risque n'est pas un expert en conformité, un concepteur de contrôles ou un gardien des politiques. Il est :

- **Un penseur systémique** qui voit des modèles et des interdépendances que les autres ne voient pas.

They must operate comfortably where data is incomplete, stakes are reputational, and decisions are as moral as they are technical.

The Required Pivot: From Control to Capability

The profession's survival depends on a fundamental reframe:

From: "Identify, assess, and mitigate risks" **To:** "Enable fast, principled, and coordinated decision-making under uncertainty"

This shift transforms risk professionals from:

- Guardians of control → Architects of organisational adaptability
- Risk avoidance → Risk navigation
- Second-line assurance → First-order decision support
- Control designers → Trust strategists and crisis translators

Your 90-Day Professional Transformation Plan

You can't transform your entire organisation overnight. But you can start demonstrating new value immediately. Here's your practical roadmap:

Days 1-30: Prove New Value

Week 1: Intelligence Demonstration

- Identify your organisation's top strategic initiative.
- Write a one-page strategic risk intelligence brief: "How the volatility landscape affects execution and opportunity"

- **Un stratège de la confiance** qui comprend comment la légitimité se construit et se perd.
- **Un traducteur de crise** qui passe sans difficulté de la profondeur technique à la clarté stratégique.
- Un **créateur de valeur** qui identifie comment la volatilité crée un avantage concurrentiel.
- Un **facilitateur d'actions fondées sur des principes** qui permet de prendre des décisions rapides lorsque la certitude est impossible.

Il doit être à l'aise dans un environnement où les données sont incomplètes, où les enjeux sont liés à la réputation et où les décisions sont autant morales que techniques.

Le pivot nécessaire : du contrôle à la capacité

La survie de la profession dépend d'un changement fondamental :

De : « Identifier, évaluer et atténuer les risques » **À :** « Permettre une prise de décision rapide, fondée sur des principes et coordonnée dans un contexte d›incertitude »

Ce changement transforme les professionnels du risque :

- Gardiens du contrôle → Architectes de l'adaptabilité organisationnelle
- Éviter les risques → Naviguer entre les risques
- Assurance de deuxième ligne → Aide à la décision de premier ordre
- Concepteurs de contrôles → Stratèges de confiance et traducteurs de crise

Votre plan de transformation professionnelle en 90 jours

Vous ne pouvez pas transformer toute votre organisation du jour au lendemain. Mais vous pouvez commencer à démontrer immédiatement une nouvelle valeur ajoutée. Voici votre feuille de route pratique :

Jours 1 à 30 : démontrer une nouvelle valeur

Semaine 1 : démonstration de l'intelligence

- Identifiez la principale initiative stratégique de votre organisation.
- Rédigez un rapport stratégique d'une page sur les risques : « Comment la volatilité du contexte affecte l'exécution et les opportunités ».
- Partagez-le spontanément avec le responsable de l'initiative.

- Share unsolicited with the initiative owner.
- Message: "I want to demonstrate how risk intelligence adds value upstream, not just reviews downstream"

Week 2: Speed Demonstration

- Document your current crisis response time for a recent event.
- Design a protocol that cuts response time by 50%
- Present to leadership: "Here's how we responded to X. Here's how we could have responded in half the time. Here's what we need to build that capability."

Week 3: Interdependency Demonstration

- Map one recent crisis retrospectively, showing all domains it touched.
- Identify connections that weren't visible beforehand.
- Present as case study: "Here's what integrated risk thinking reveals that siloed approaches miss"

Week 4: Scenario Demonstration

- Design one compound scenario (multiple simultaneous crises)
- Facilitate a 90-minute tabletop exercise with leadership.
- Focus on discovering interdependencies and decision tensions.
- Capture: "Here's what we learned about our coherence under compound pressure"

Goal: Demonstrate that you can provide strategic value, not just compliance assurance.

Days 31-60: Build New Capabilities

Personal development sprint:

- Enrol in an advanced data analytics or AI course
- Read three books on business strategy (not risk management)
- Practice storytelling: Record yourself presenting risk intelligence, watch back, and refine
- Shadow someone in strategy or communications for a day.

- Message : « Je souhaite démontrer comment l'intelligence en matière de risques ajoute de la valeur en amont, et ne se limite pas à des analyses en aval ».

Semaine 2 : Démonstration de rapidité

- Documentez votre temps de réponse actuel à une crise récente.
- Concevez un protocole qui réduit le temps de réponse de 50 %.
- Présentez-le à la direction : « Voici comment nous avons réagi à X. Voici comment nous aurions pu réagir en deux fois moins de temps. Voici ce dont nous avons besoin pour développer cette capacité. »

Semaine 3 : Démonstration de l'interdépendance

- Cartographiez rétrospectivement une crise récente en montrant tous les domaines qu'elle a touchés.
- Identifiez les liens qui n'étaient pas visibles auparavant.
- Présentez sous forme d'étude de cas : « Voici ce que la réflexion intégrée sur les risques révèle et que les approches cloisonnées ne permettent pas de voir ».

Semaine 4 : Démonstration de scénario

- Concevez un scénario complexe (plusieurs crises simultanées).
- Animez un exercice de simulation de 90 minutes avec les dirigeants.
- Concentrez-vous sur la découverte des interdépendances et des tensions décisionnelles.
- Conclusion : « Voici ce que nous avons appris sur notre cohérence sous une pression complexe ».

Objectif : démontrer que vous pouvez apporter une valeur stratégique, et pas seulement une assurance de conformité.

Jours 31 à 60 : développer de nouvelles capacités

Sprint de développement personnel :

- Inscrivez-vous à un cours avancé sur l'analyse de données ou l'IA
- Lisez trois livres sur la stratégie d'entreprise (et non sur la gestion des risques)

- Attend an executive presentation workshop.

Infrastructure building:

- Build a prototype "always-on" dashboard for one risk domain.
- Draft crisis decision authority matrix
- Conduct the first values stress-test session with a willing leader.
- Create a crisis activation protocol with timing targets

Relationship building:

- Schedule coffee with heads of Strategy, Communications, and Operations.
- Message: "I want to understand how risk intelligence could be more valuable to your work"
- Listen more than you talk.
- Identify integration opportunities

Goal: Develop the capabilities and relationships for sustained transformation.

Days 61-90: Scale and Formalise

Framework adoption:

- Present the SRR Framework (or adapted version) to your leadership.
- Propose pilot implementation focused on the highest-value use case.
- Secure budget and authority for one major capability build (monitoring system, scenario program, training initiative)

Metric transformation:

- Propose new performance indicators focused on resilience outcomes: Speed of escalation, decision coher-

- Entraînez-vous à raconter des histoires : enregistrez-vous en train de présenter des informations sur les risques, regardez l'enregistrement et affinez votre présentation
- Suivez quelqu'un dans le domaine de la stratégie ou de la communication pendant une journée.
- Participez à un atelier de présentation pour cadres.

Mise en place d'une infrastructure :

- Construisez un prototype de tableau de bord « toujours actif » pour un domaine de risque.
- Rédigez une matrice des pouvoirs décisionnels en cas de crise.
- Organisez la première session de test de résistance des valeurs avec un dirigeant volontaire.
- Créer un protocole d'activation en cas de crise avec des objectifs de timing.

Établissement de relations :

- Organiser un café avec les responsables de la stratégie, de la communication et des opérations.
- Message : « Je souhaite comprendre en quoi les informations sur les risques pourraient être plus utiles à votre travail ».
- Écoutez plus que vous ne parlez.
- Identifier les opportunités d'intégration

Objectif : développer les capacités et les relations nécessaires à une transformation durable.

Jours 61 à 90 : Déployer et formaliser

Adoption du cadre :

- Présentez le cadre SRR (ou une version adaptée) à vos dirigeants.
- Proposer une mise en œuvre pilote axée sur le cas d'utilisation présentant la plus grande valeur ajoutée.
- Obtenir le budget et l'autorisation nécessaires pour la mise en place d'une capacité majeure (système de surveillance, programme de scénarios, initiative de formation).

Transformation des indicateurs :

- Proposer de nouveaux indicateurs de performance axés sur les résultats en matière de résilience : rapidité de l'escalade, cohérence des décisions, temps de rétablissement de la confiance et capture de l'avantage concurrentiel.

ence, trust recovery time, and competitive advantage capture.

- Show how these better reflect actual value than traditional metrics.

Strategic positioning:

- Request a role clarification conversation with your executive sponsor.
- Topic: "I want to understand how risk can be positioned as a more strategic partner, less compliance function. What would make risk intelligence indispensable to you?"
- Based on feedback, propose a pilot "embedded risk strategist" model where you join one strategic initiative from inception.

Goal: Formalise your transformation and create organisational pull for a new model.

The Uncomfortable Questions You Must Answer

Before you dismiss this as "not applicable to my organisation" or "my leadership won't support this," ask yourself these questions honestly:

1. Am I confusing activity with impact? I'm busy. I have meetings. I produce reports. But am I in the room when decisions that matter are being made? Or am I finding out about them afterwards?

2. Am I defending a methodology because it's comfortable? Do I advocate for traditional approaches because they're genuinely most effective, or because they're what I know and changing feels risky?

3. Am I hiding behind "organisational constraints"? Do I blame my organisation for not valuing risk, or have I failed to demonstrate value in the language leadership understands?

4. Would my organisation be measurably worse off if my role disappeared tomorrow? Not "would processes be missed"—would actual decision quality and organisational resilience be meaningfully diminished?

5. Am I becoming obsolete and refusing to see it? Are other functions (strategy, communications, operations) increasingly making risk decisions without me? Am I being invited to fewer important conversations than I was two years ago?

- Montrer en quoi ceux-ci reflètent mieux la valeur réelle que les indicateurs traditionnels.

Positionnement stratégique :

- Demandez à votre sponsor exécutif de clarifier votre rôle.
- Sujet : « Je souhaite comprendre comment le risque peut être positionné comme un partenaire plus stratégique et moins comme une fonction de conformité. Qu'est-ce qui rendrait l'intelligence du risque indispensable à vos yeux ? »
- Sur la base des commentaires reçus, proposez un modèle pilote de « stratège en gestion des risques intégré » dans lequel vous participez à une initiative stratégique dès sa création.

Objectif : formaliser votre transformation et créer une dynamique organisationnelle en faveur d'un nouveau modèle.

Les questions dérangeantes auxquelles vous devez répondre

Avant de rejeter cette idée en disant « cela ne s'applique pas à mon organisation » ou « mes dirigeants ne soutiendront pas cela », posez-vous honnêtement les questions suivantes :

1. Est-ce que je confonds activité et impact ? Je suis occupé. J'ai des réunions. Je produis des rapports. Mais suis-je présent lorsque des décisions importantes sont prises ? Ou est-ce que je les découvre après coup ?

2. Est-ce que je défends une méthodologie parce qu'elle me convient ? Est-ce que je préconise les approches traditionnelles parce qu'elles sont vraiment les plus efficaces, ou parce que ce sont celles que je connais et que le changement me semble risqué ?

3. Est-ce que je me cache derrière les « contraintes organisationnelles » ? Est-ce que je reproche à mon organisation de ne pas valoriser le risque, ou est-ce que je n'ai pas réussi à démontrer la valeur de mon travail dans un langage compréhensible par la direction ?

4. Mon organisation serait-elle nettement moins performante si mon rôle disparaissait demain ? Je ne parle pas de « processus manquants », mais bien d'une diminution significative de la qualité des décisions et de la résilience organisationnelle.

If any of these questions make you uncomfortable, that discomfort is information. Pay attention to it.

The Fork in the Road

Here's where we are: The profession of risk management is at an inflection point.

One path leads to continued relevance, professional growth, strategic partnership, and career advancement. Risk professionals on this path become organisational architects of resilience, trusted advisors who help leadership navigate permanent uncertainty while capturing competitive advantage from volatility others cannot manage.

The other path leads to slow marginalisation, perceived commodity value, and potential elimination through automation or consolidation. Risk professionals on this path become procedural historians – documenting failure rather than shaping success.

The uncomfortable reality is that **most risk professionals are currently on the second path, and many don't realise it yet.**

The even more uncomfortable reality is that **changing paths requires you to change first, before your organisation changes.**

You can't wait for your leadership to recognise that they need you to be more strategic. You must demonstrate strategic value so compellingly that they can't imagine operating without it.

You can't wait for your organisation to redesign your role. You must show what the redesigned role delivers so clearly that they formalise what you've been proving informally.

You can't wait for permission to develop new capabilities. You must build them on your own time and demonstrate their value in your current role.

5. Suis-je en train de devenir obsolète et refuse-je de le voir ? D'autres fonctions (stratégie, communication, opérations) prennent-elles de plus en plus de décisions en matière de risque sans moi ? Suis-je invité à moins de conversations importantes qu'il y a deux ans ?

Si l'une de ces questions vous met mal à l'aise, ce malaise est une information. Soyez-y attentif.

À la croisée des chemins

Voici où nous en sommes : la profession de gestionnaire de risques est à un tournant.

Une voie mène à une pertinence continue, à une croissance professionnelle, à un partenariat stratégique et à une progression de carrière. Les professionnels du risque qui empruntent cette voie deviennent les architectes de la résilience organisationnelle, des conseillers de confiance qui aident les dirigeants à naviguer dans une incertitude permanente tout en tirant parti de la volatilité que d'autres ne peuvent gérer.

L'autre voie mène à une marginalisation lente, à une perception de valeur marchande et à une élimination potentielle par l'automatisation ou la consolidation. Les professionnels du risque qui empruntent cette voie deviennent des historiens des procédures, documentant les échecs plutôt que façonnant le succès.

La réalité inconfortable est que **la plupart des professionnels du risque se trouvent actuellement sur la deuxième voie, et beaucoup ne s'en rendent pas encore compte.**

La réalité encore plus inconfortable est que **pour changer de voie, vous devez d'abord changer vous-même, avant que votre organisation ne change.**

Vous ne pouvez pas attendre que vos dirigeants reconnaissent qu'ils ont besoin que vous soyez plus stratégique. Vous devez démontrer votre valeur stratégique de manière si convaincante qu'ils ne peuvent imaginer fonctionner sans elle.

Vous ne pouvez pas attendre que votre organisation redéfinisse votre rôle. Vous devez montrer si clairement ce que le rôle redéfini apporte qu'ils officialisent ce que vous avez prouvé de manière informelle.

Vous ne pouvez pas attendre d'avoir la permission de développer de nouvelles compétences. Vous devez les acquérir pendant votre temps libre et démontrer leur valeur dans votre rôle actuel.

C'est la dure réalité de la transformation professionnelle : c'est à vous de faire le premier pas.

This is the hard truth about professional transformation: you go first.

A Final Provocation

Let me end where I began, with uncomfortable directness: The risk management profession doesn't have a future. **Risk strategists and organisational resilience architects** have a future.

Risk strategists and organisational resilience architects have a future.

The question is whether you make that transition, or whether someone else – from strategy, from communications, from data science, from operations – makes it faster than you and takes the role that should have been yours.

In a polycrisis world, organisations desperately need people who can help them navigate continuous uncertainty with speed, coherence, and competitive advantage. They need strategic partners who see around corners, connect dots others miss, and enable principled action when certainty is impossible.

They will find those people. **The question is whether those people are risk professionals who evolved, or other professionals who learned risk thinking faster than risk professionals learned strategic thinking.**

The risk profession is dying. But an opportunity is being born.

Which side of that transition will you be on?

Act Now

If this resonates, here's what to do today:

1. **Audit yourself**: Score your capabilities across technical (AI, analytics) and human (judgment, communication) dimensions. Identify gaps.
2. **Demonstrate value**: Pick one strategic initiative. Write that one-page intelligence brief. Share it unsolicited. Start proving new value.
3. **Build one capability**: Choose the SRR Framework pillar where you're weakest. Commit to building basic capability in 30 days.

Une dernière provocation

Je terminerai comme j'ai commencé, avec une franchise dérangeante : la profession de gestionnaire de risques n'a pas d'avenir. **Les stratèges en matière de risques et les architectes de la résilience organisationnelle** ont un avenir.

Les stratèges en matière de risques et les architectes de la résilience organisationnelle ont un avenir.

La question est de savoir si vous effectuez cette transition ou si quelqu'un d'autre – issu de la stratégie, de la communication, de la science des données, des opérations – le fait plus rapidement que vous et prend le rôle qui aurait dû être le vôtre.

Dans un monde en proie à de multiples crises, les organisations ont désespérément besoin de personnes capables de les aider à naviguer dans l'incertitude permanente avec rapidité, cohérence et avantage concurrentiel. Elles ont besoin de partenaires stratégiques qui voient plus loin, relient les points que d'autres ne voient pas et permettent d'agir de manière réfléchie lorsque la certitude est impossible.

Elles trouveront ces personnes. **La question est de savoir si ces personnes sont des professionnels du risque qui ont évolué, ou d'autres professionnels qui ont appris à penser en termes de risque plus rapidement que les professionnels du risque n'ont appris à penser en termes de stratégie.**

La profession de gestionnaire de risques est en train de mourir. Mais une opportunité est en train de naître.

De quel côté de cette transition vous situerez-vous ?

Agissez dès maintenant

Si cela vous interpelle, voici ce que vous pouvez faire dès aujourd'hui :

1. **Évaluez-vous** : évaluez vos capacités sur les plans technique (IA, analyse) et humain (jugement, communication). Identifiez vos lacunes.
2. **Démontrez votre valeur** : choisissez une initiative stratégique. Rédigez un rapport d'information d'une page. Partagez-le spontanément. Commencez à prouver votre nouvelle valeur.
3. **Développez une compétence** : choisissez le pilier du cadre SRR dans lequel vous êtes le plus faible. Engagez-vous à développer cette compétence de base en 30 jours.

4. **Have one conversation**: Schedule time with your executive sponsor or CEO. Ask: "How could risk intelligence become more valuable to your decision-making?"

5. **Connect with peers**: Find risk professionals who are navigating this transformation. Share learning. Build community.

The future of risk management is being written right now. How you respond to this moment will determine your future.

Let's build the future of the risk profession together. Ω

4. **Ayez une conversation** : prenez rendez-vous avec votre sponsor exécutif ou votre PDG. Demandez-lui : « Comment l'intelligence des risques pourrait-elle devenir plus utile à votre prise de décision ? »

5. **Entrez en contact avec vos pairs** : trouvez des professionnels du risque qui mènent cette transformation. Partagez vos connaissances. Créez une communauté.

L'avenir de la gestion des risques s'écrit en ce moment même. La manière dont vous réagissez à ce moment déterminera votre avenir.

Construisons ensemble l'avenir de la profession de gestionnaire de risques. Ω

ABOUT THE AUTHOR

Patrick Ow is a Melbourne-based risk and resilience specialist who focuses on using risk management strategically to help organizations navigate continuous uncertainty and compound disruptions.

He advocates for risk professionals to act as architects of organizational resilience and adaptability, supporting leaders as trusted strategists in responding to uncertainty, achieving strategic objectives, and capturing value from volatility.

Patrick's work is grounded in the belief that the future of risk management lies not in avoidance or control, but in enabling organizations to anticipate change, respond decisively, and recover stronger after disruption.

As a Chartered Accountant and Risk Specialist with over 25 years of international risk management and corporate governance experience in the private, not-for-profit, and public sectors, he helps individuals and organizations make better decisions to achieve better results as a corporate and personal trainer and coach.

https://www.linkedin.com/in/patrickow/

À PROPOS DE L'AUTEUR

Patrick Ow est un spécialiste des risques et de la résilience basé à Melbourne qui se concentre sur l'utilisation stratégique de la gestion des risques pour aider les organisations à faire face à l'incertitude permanente et aux perturbations complexes.

Il encourage les professionnels du risque à agir en tant qu'architectes de la résilience et de l'adaptabilité organisationnelles, en aidant les dirigeants, en tant que stratèges de confiance, à répondre à l'incertitude, à atteindre les objectifs stratégiques et à tirer parti de la volatilité.

Le travail de Patrick repose sur la conviction que l'avenir de la gestion des risques ne réside pas dans l'évitement ou le contrôle, mais dans la capacité des organisations à anticiper le changement, à réagir de manière décisive et à se relever plus fortes après une perturbation.

En tant que comptable agréé et spécialiste des risques, fort de plus de 25 ans d'expérience internationale en gestion des risques et en gouvernance d'entreprise dans les secteurs privé, public et à but non lucratif, il aide les particuliers et les organisations à prendre de meilleures décisions pour obtenir de meilleurs résultats en tant que formateur et coach d'entreprise et personnel.

AMAZING CANADIAN EXERCISE

Empowering Canada's continuity professionals to build around resilient nation

INCROYABLE EXERCISE CANADIENNE

DRI CANADA Train. Prepare. Recover.

DRI CANADA'S YEAR OF EXERCISE DESIGN

The Amazing Canadian Exercise

A National Tabletop Challenge

In an era where cyber threats loom large over national infrastructure, DRI Canada is taking a bold step to help strengthen organizational resilience. The initiative, titled The Amazing Canadian Exercise, is a gamified, national tabletop challenge designed to test and elevate the readiness of organizations across the country.

The Scenario

Over six months, participants will be presented with a simulated, state-sponsored cyber-attack targeting Canadian critical infrastructure, with the scenario escalating in complexity and impact as time progresses.

Purpose and Strategic Vision

The challenge is not just a game; it's a rigorous professional development exercise.

L'incroyable exercice canadienne

Un défi national sur table

À une époque où les cybermenaces pèsent lourdement sur les infrastructures nationales, DRI Canada prend une mesure audacieuse pour aider à renforcer la résilience des organisations. L›initiative, intitulée « L›incroyable catastrophe canadienne », est un défi national ludique conçu pour tester et améliorer la préparation des organisations à travers le pays.

Le scénario

Pendant six mois, les participants seront confrontés à une simulation de cyberattaque commanditée par un État et visant les infrastructures critiques canadiennes, le scénario gagnant en complexité et en impact au fil du temps.

Its core purpose is to move organizations beyond static tabletop discussions, fostering sustained, scenario-driven response and continuous improvement.

By aligning with DRI International Professional Practices, the program encourages high-quality tabletop best practices, cross-functional collaboration, and leadership decision-making. It also aims to demonstrate how such exercises can generate measurable outcomes, create national engagement, and provide a scalable model for future professional development.

Structure and Participation

Teams of four to six participants, with at least half being DRI certified professionals, are invited to join. The challenge is open to both certified and non-certified practitioners, and encourages cross-functional teams from business continuity, IT, cyber, communications, risk, and leadership backgrounds. Each month, teams receive a structured "inject package" and must submit their response within a defined window, simulating the evolving nature of a real crisis.

The Scenario: Six Months of Escalation

The heart of the challenge is a progressive scenario that unfolds over six months:

- **Month 1:** Detection & Initial Response, teams must recognize incidents and make early decisions amid conflicting information.
- **Month 2:** Escalation & Coordination, broader impacts and third-party concerns emerge, requiring external coordination.
- **Month 3:** Leadership & Crisis Communications, executive decisions and media pressure test internal and external communications.
- **Month 4:** Sustained Operations, prolonged disruption and resource constraints challenge continuity.
- **Month 5:** Recovery & Improvement, focus shifts to restoration and learning from the crisis.
- **Month 6:** Assurance & Governance, teams measure effectiveness and assess program maturity, preparing for future incidents.

Objectif et vision stratégique

Ce défi n'est pas seulement un jeu, c'est un exercice de développement professionnel rigoureux.

Son objectif principal est d'amener les organisations à dépasser les discussions statiques autour d'une table, en favorisant une réponse durable, basée sur des scénarios, et une amélioration continue.

En s'alignant sur les pratiques professionnelles internationales de DRI, le programme encourage les meilleures pratiques de haute qualité, la collaboration interfonctionnelle et la prise de décision par les dirigeants. Il vise également à démontrer comment de tels exercices peuvent générer des résultats mesurables, susciter l'engagement national et fournir un modèle évolutif pour le développement professionnel futur.

Structure et participation

Des équipes de quatre à six participants, dont au moins la moitié sont des professionnels certifiés par DRI, sont invitées à participer. Le défi est ouvert aux praticiens certifiés et non certifiés, et encourage la formation d'équipes interfonctionnelles issues des domaines de la continuité des activités, de l'informatique, de la cybersécurité, des communications, des risques et du leadership. Chaque mois, les équipes reçoivent un « paquet d'injection » structuré et doivent soumettre leur réponse dans un délai défini, simulant ainsi la nature évolutive d'une crise réelle.

Evaluation and Recognition

Submissions are judged by a national panel of senior resilience professionals, government representatives, and cyber subject-matter experts. Criteria include alignment to professional practices, decision-making quality, communication effectiveness, risk awareness, realism, and evidence of learning. Monthly scores and feedback drive progression, with an emphasis on learning rather than elimination.

Top teams earn recognition, including symposium registration or private courses, and all participants receive certificates, continuing education points and public acknowledgment.

Evaluation Criteria

Submissions are evaluated by the panel using a set of weighted criteria designed to ensure a fair and comprehensive assessment. The key evaluation criteria are:

- **Alignment to Professional Practices:** How well the team's response follows established professional standards and best practices.
- **Quality of Decision-Making:** The soundness, logic, and effectiveness of the decisions made throughout the scenario.

Le scénario : six mois d'escalade

Le cœur du défi est un scénario progressif qui se déroule sur six mois :

- **Mois 1 :** Détection et réponse initiale, les équipes doivent reconnaître les incidents et prendre des décisions rapides malgré des informations contradictoires.
- **Mois 2 :** Escalade et coordination, des répercussions plus larges et des préoccupations de tiers apparaissent, nécessitant une coordination externe.
- **Mois 3 :** Leadership et communication de crise, les décisions de la direction et la pression des médias mettent à l'épreuve les communications internes et externes.
- **Mois 4 :** opérations soutenues, les perturbations prolongées et les contraintes en matière de ressources remettent en question la continuité.
- **Mois 5 :** Rétablissement et amélioration, l'accent est mis sur la restauration et les enseignements tirés de la crise.
- **Mois 6 :** Assurance et gouvernance, les équipes mesurent l'efficacité et évaluent la maturité du programme, se préparant à de futurs incidents.

Évaluation et reconnaissance

Les candidatures sont évaluées par un jury national composé de professionnels chevronnés en matière de résilience, de représentants du gouvernement et d'experts en cybersécurité. Les critères d'évaluation comprennent la conformité aux pratiques professionnelles, la qualité de la prise de décision, l'efficacité de la communication, la conscience des risques, le réalisme et les preuves d'apprentissage. Les notes mensuelles et les commentaires favorisent la progression, l'accent étant mis sur l'apprentissage plutôt que sur l'élimination.

Les meilleures équipes sont récompensées, notamment par une inscription à un symposium ou à des cours privés, et tous les participants reçoivent des certificats, des points de formation continue et une reconnaissance publique.

Critères d'évaluation

Les candidatures sont évaluées par le jury à l'aide d'un ensemble de critères pondérés conçus pour garantir une évaluation équitable et complète. Les principaux critères d'évaluation sont les suivants

- **Conformité aux pratiques professionnelles :** dans quelle mesure la réponse de l'équipe respecte-t-elle les normes professionnelles établies et les meilleures pratiques ?

- **Clarity and Effectiveness of Communications:** How clearly and effectively the team communicates both internally and externally during the crisis.
- **Risk Awareness and Prioritization:** The team's ability to identify, assess, and prioritize risks as the scenario unfolds.
- **Practicality and Realism:** The feasibility and realism of the proposed actions and strategies.
- **Evidence of Learning and Adaptation Over Time:** Demonstrated improvement, learning, and adaptation as the scenario progresses month by month.

Teams receive monthly scores and qualitative feedback based on these criteria, with aggregate scoring across all six months. The emphasis is on learning and continuous improvement, rather than elimination.

Board-Level Value and National Impact

This initiative reinforces DRI Canada's leadership in experiential professional development, advances consistent application of professional practices, and creates national visibility. It supports certification credibility and employer value, offering a scalable model for future challenges. Importantly, the exercise is clearly labeled as simulated, uses no sensitive information, and maintains a sector-neutral design for broad applicability

In summary: The Amazing Canadian Exercise is more than a competition, it's a transformative experience for Canadian organizations, blending realism, collaboration, and continuous learning to prepare for the cyber threats of tomorrow.

Six Months. One Crisis.
How Will You Respond? *- G.A.T.* Ω

- **Qualité de la prise de décision :** le bien-fondé, la logique et l'efficacité des décisions prises tout au long du scénario.
- **Clarté et efficacité de la communication :** la clarté et l'efficacité avec lesquelles l'équipe communique en interne et en externe pendant la crise.
- **Conscience des risques et hiérarchisation :** capacité de l'équipe à identifier, évaluer et hiérarchiser les risques au fur et à mesure que le scénario se déroule.
- **Caractère pratique et réalisme :** faisabilité et réalisme des actions et stratégies proposées.
- **Preuve d'apprentissage et d'adaptation au fil du temps :** amélioration, apprentissage et adaptation démontrés au fur et à mesure que le scénario progresse mois après mois.

Les équipes reçoivent des notes mensuelles et des commentaires qualitatifs basés sur ces critères, avec une note globale sur les six mois. L'accent est mis sur l'apprentissage et l'amélioration continue, plutôt que sur l'élimination.

Valeur au niveau du conseil d'administration et impact national

Cette initiative renforce le leadership de DRI Canada en matière de développement professionnel expérientiel, favorise l'application cohérente des pratiques professionnelles et crée une visibilité nationale. Elle soutient la crédibilité de la certification et la valeur pour les employeurs, en offrant un modèle évolutif pour les défis futurs. Il est important de noter que l'exercice est clairement présenté comme une simulation, n'utilise aucune information sensible et conserve une conception neutre sur le plan sectoriel pour une large applicabilité.

En résumé : The Amazing Canadian Disaster est plus qu'une simple compétition, c'est une expérience transformatrice pour les organisations canadiennes, alliant réalisme, collaboration et apprentissage continu afin de se préparer aux cybermenaces de demain.

Six mois. Une crise.
Comment allez-vous réagir ? *- G.A.T.* Ω

Breaking News: Canada Faces Unprecedented National Power Disruption – DRI Canada's The Amazing Canadian Exercise Begins

In an unprecedented event unfolding across Canada, millions are experiencing widespread power outages as a **cascading failure hits the national electricity grid**. Within 45 minutes, over **70% of Canadians are without power**, and major urban centres are reporting rolling or sustained blackouts. Telecommunications networks are rapidly degrading, leaving communities struggling to access reliable information.

Early technical assessments indicate this is not a standard equipment failure. Initial reports suggest a **hostile cyber operation targeting operational technology (OT) and grid management systems**, designed to disrupt infrastructure rather than steal or destroy data. Analysts warn that the cascading effects are **unlike anything seen before in Canadian history**, affecting hospitals, transit systems, water supply, and financial services.

Dernières nouvelles : Le Canada confronté à une panne d'électricité nationale sans précédent – Le grand exercice canadien de DRI Canada commence

Dans un événement sans précédent qui se déroule à travers le Canada, des millions de personnes sont touchées par des pannes d'électricité généralisées alors qu'une **défaillance en cascade frappe le réseau électrique national**. En l'espace de 45 minutes, plus **de 70 % des Canadiens se retrouvent sans électricité**, et les grands centres urbains signalent des pannes d'électricité intermittentes ou prolongées. Les réseaux de télécommunications se détériorent rapidement, laissant les communautés dans l'incapacité d'accéder à des informations fiables.

Les premières évaluations techniques indiquent qu'il ne s'agit pas d'une panne d'équipement classique. Les rapports initiaux suggèrent qu'il s'agit d'une **cyberopération**

Public Reaction and Misinformation

As citizens adjust to the sudden blackout, misinformation is spreading across social media, complicating situational awareness for both authorities and the public. Emergency services are operating under extreme conditions, with backup power systems stretched to their limits. Communities are coming together, showing resilience and resourcefulness, but the scale of the disruption is testing every level of society—from businesses and local governments to individual households.

Pausing this breaking news….

A National Exercise in Real Time

Introducing DRI Canada's – **The Amazing Canadian Exercise**, a unique national resilience challenge designed to test Canadian businesses and communities' capacity to respond to complex, cascading disruptions.

This scenario was created to **stress-test critical operations under realistic, high-pressure conditions**, providing organizations with the opportunity to evaluate their strategies, coordination, and decision-making under uncertainty.

"This exercise goes beyond traditional business continuity drills," says Garth Tucker, Editor of True North Resilience. "It challenges organizations and communities to respond in a scenario where **infrastructure, technology, workforce capacity, public trust, and social stability are all under pressure simultaneously.** The goal is not to identify 'right' or 'wrong' decisions, it's to strengthen resilience at every level."

hostile ciblant les technologies opérationnelles (OT) et les systèmes de gestion du réseau, conçue pour perturber les infrastructures plutôt que pour voler ou détruire des données. Les analystes avertissent que les effets en cascade sont **sans précédent dans l'histoire du Canada** et affectent les hôpitaux, les réseaux de transport, l'approvisionnement en eau et les services financiers.

Réaction du public et désinformation

Alors que les citoyens s'adaptent à cette panne soudaine, la désinformation se répand sur les réseaux sociaux, compliquant la compréhension de la situation tant pour les autorités que pour le public. Les services d'urgence fonctionnent dans des conditions extrêmes, les systèmes d'alimentation de secours étant poussés à leurs limites. Les communautés se serrent les coudes, faisant preuve de résilience et d'ingéniosité, mais l'ampleur des perturbations met à l'épreuve tous les niveaux de la société, des entreprises et des administrations locales aux ménages individuels.

Mise en pause de l' s sur cette actualité brûlante...

Un exercice national en temps réel

Présentation de DRI Canada – **The Amazing Canadian Exercise**, un défi national unique en matière de résilience, conçu pour tester la capacité des entreprises et des communautés canadiennes à répondre à des perturbations complexes et en cascade.

Ce scénario a été créé pour **tester la résistance des opérations critiques dans des conditions réalistes et sous haute pression**, offrant aux organisations la possibilité d'évaluer leurs stratégies, leur coordination et leur prise de décision dans un contexte d'incertitude.

« Cet exercice va au-delà des exercices traditionnels de continuité des activités », explique Garth Tucker, Redacteur en Chef de True North Resilience. « Il met au défi les organisations et les communautés de réagir dans un scénario où **les infrastructures, la technologie, la capacité de main-d'œuvre, la confiance du public et la stabilité sociale sont toutes soumises à des pressions simultanées.** L'objectif n'est pas d'identifier les « bonnes » ou les « mauvaises » décisions, mais de renforcer la résilience à tous les niveaux. »

Critical Decisions Under Pressure

Participants in the exercise are encouraged to:

Accept the Scenario: Focus on understanding the disruption rather than debating its likelihood.

Take Inventory: Assess available resources and consider immediate and cascading impacts.

Collaborate: Coordinate across departments, sectors, and community groups to ensure continuity of essential operations.

Learn and Adapt: Identify gaps, test decision-making processes, and improve response capabilities for real-world disruptions.

The exercise highlights the **interconnected-ness of Canadian society**: a failure in one sector, like power, quickly affects telecommunications, transportation, healthcare, and public confidence. By simulating these pressures, organizations gain insight into **how decisions ripple across complex systems** and what actions strengthen resilience under extreme conditions.

Looking Ahead: Building National Resilience

The Amazing Canadian Exercise is more than a drill; it is a **call to action for all Canadians**. As the nation faces rapidly evolving threats in the cyber-physical domain, resilience is no longer optional—it is a **collective capability essential for national security, economic stability, and public safety**.

Décisions critiques sous pression

Les participants à l'exercice sont encouragés à :

Accepter le scénario : se concentrer sur la compréhension de la perturbation plutôt que de débattre de sa probabilité.

Faire l'inventaire : évaluer les ressources disponibles et examiner les répercussions immédiates et en cascade.

Collaborer : coordonner les efforts entre les départements, les secteurs et les groupes communautaires afin d'assurer la continuité des opérations essentielles.

Apprendre et s'adapter : identifier les lacunes, tester les processus décisionnels et améliorer les capacités de réponse aux perturbations dans le monde réel.

L'exercice met en évidence **l'interdépendance de la société canadienne** : une défaillance dans un secteur, comme celui de l'électricité, affecte rapidement les télécommunications, les transports, les soins de santé et la confiance du public. En simulant ces pressions, les organisations acquièrent une meilleure compréhension de **la manière dont les décisions se répercutent sur des systèmes complexes** et des mesures qui renforcent la résilience dans des conditions extrêmes.

Perspectives d'avenir : renforcer la résilience nationale

L'exercice Amazing Canadian est plus qu'un simple exercice ; c'est un **appel à l'action pour tous les Canadiens**. Alors que le pays est confronté à des menaces en constante évolution dans le domaine cyberphysique, la résilience n'est plus une option, mais une **capacité collective essentielle à la sécurité nationale, à la stabilité économique et à la sécurité publique**.

How to get involved

Register a team (4-6 people) and test your organization's programs or use our fictional company. The exercise runs from May to November 2026, with monthly injects as the situation unfolds. Each team will submit their response monthly, judged by a panel comprised of national representatives.

Entry forms are available from:

The DRI Canada website: www.dri.ca

Email: tace@dri.ca Ω

Comment participer

Inscrivez une équipe (4 à 6 personnes) et testez les programmes de votre organisation ou utilisez notre entreprise fictive. L'exercice se déroulera de mai à novembre 2026, avec des injections mensuelles au fur et à mesure que la situation évoluera. Chaque équipe soumettra sa réponse chaque mois, qui sera évaluée par un jury composé de représentants nationaux.

Les formulaires d'inscription sont disponibles sur :

Le site web de DRI Canada : www.dri.ca

Courriel : tace@dri.ca Ω

ABOUT THE AUTHOR

***Perry Ruehlen**, ASSP CE is an experienced association executive with over 20 years of success helping non-profit boards achieve their strategic goals and operate with organizational excellence. Throughout her career, she has partnered with associations ranging from 50 to over 7,000 members, delivering comprehensive management solutions that strengthen governance, enhance member engagement, and drive long-term sustainability.*

Perry's expertise spans member services, board governance, certification programs, educational delivery, professional development, and conference planning. She takes pride in fostering collaborative relationships with board members—enabling them to lead confidently as subject matter experts while ensuring the operational and strategic foundations are strong.

À PROPOS DE L'AUTEUR

***Perry Ruehlen**, ASSP CE, est une dirigeante expérimentée qui aide depuis plus de 20 ans les conseils d'administration d'organisations à but non lucratif à atteindre leurs objectifs stratégiques et à fonctionner avec excellence sur le plan organisationnel. Tout au long de sa carrière, elle a collaboré avec des associations comptant de 50 à plus de 7 000 membres, leur fournissant des solutions de gestion complètes qui renforcent la gouvernance, améliorent l'engagement des membres et favorisent la viabilité à long terme.*

L'expertise de Perry couvre les services aux membres, la gouvernance des conseils d'administration, les programmes de certification, la formation, le développement professionnel et la planification de conférences. Elle est fière de favoriser les relations de collaboration avec les membres des conseils d'administration, leur permettant ainsi de diriger en toute confiance en tant qu'experts dans leur domaine tout en garantissant la solidité des fondements opérationnels et stratégiques.

Upcoming Event

DRI Canada is dedicated to providing continued professional development for its certified professionals through a variety of opportunities - whether it be one day, one hour or one lunch.

DRIC symposiums are one-day events specifically designed for senior-level business continuity, disaster recovery, cyber resilience and risk management professionals. They aim to provide a dynamic and interactive platform for leaders to explore innovative strategies, share best practices, and discuss the latest trends in business continuity management.

During these immersive events, participants can engage with like-minded professionals and thought leaders from diverse sectors. The symposium will foster collaboration and knowledge exchange, enabling attendees to enhance their skill sets and stay ahead in the rapidly evolving field of business continuity.

Upcoming Date

April 16, 2026 Toronto, ON

Log in and register for events at:
https://www.dri.ca/events.php

Événement à venir

DRI Canada s'engage à offrir un perfectionnement professionnel continu à ses professionnels certifiés grâce à une variété d'occasions, qu'il s'agisse d'une journée, d'une heure ou d'un déjeuner.

Les symposiums DRIC sont des événements d'une journée spécialement conçus pour les professionnels de haut niveau dans les domaines de la continuité des activités, de la reprise après sinistre, de la cyber-résilience et de la gestion des risques. Ils visent à fournir une plateforme dynamique et interactive permettant aux dirigeants d'explorer des stratégies innovantes, de partager les meilleures pratiques et de discuter des dernières tendances en matière de gestion de la continuité des activités.

Au cours de ces événements immersifs, les participants peuvent échanger avec des professionnels partageant les mêmes idées et des leaders d'opinion issus de divers secteurs. Le symposium favorisera la collaboration et l'échange de connaissances, permettant aux participants d'améliorer leurs compétences et de rester à la pointe dans le domaine en rapide évolution de la continuité des activités.

Date à venir

16 avril 2026 Toronto, ON

Connectez-vous et inscrivez-vous aux événements sur :
https://www.dri.ca/events.php

SUPPLY CHAIN RISK
RISQUE LIÉ À LA CHAÎNE D'APPROVISIONNEMENT

By/Par ***Seema Verma*** *CBCP, BCCE, LA ISO 2 3301:2019, LA ISO 27001*

Supply Chain Risk - No Organization Is Resilient Alone – Only Ecosystems Are

Today's global world is the world of interlocking systems and interdependent organizations. Will it be correct if stated "My business is resilient" or "XYZ is resilient"?

Any business or organization is a complex network of multiple systems and subsystems, and these systems constantly interact with one another. Business interacts with other businesses, vendors, the government, public systems, etc.

To remain relevant in business, most of these vendors and sub-vendors will (and should) have the capability to anticipate, adapt, and improvise during and after a disruption.

Hence, the resilience of any organization or business is the result of or is dependent on the challenged system's interaction with others during the disruption. Every organization or business is both resilient and vulnerable, at the same time, depending on the state of other organizations, systems, or vendors with which it interacts.

Resilience is the process that will put to the test the continuity strategies of

Risque lié à la chaîne d'approvisionnement - Aucune organisation n'est résiliente à elle seule, seuls les écosystèmes le sont

Le monde globalisé d'aujourd'hui est un monde de systèmes interdépendants et d'organisations interdépendantes. Est-il correct d'affirmer que « mon entreprise est résiliente » ou que « XYZ est résiliente » ?

Toute entreprise ou organisation est un réseau complexe composé de multiples systèmes et sous-systèmes, et ces systèmes interagissent constamment les uns avec les autres. Les entreprises interagissent avec d'autres entreprises, des fournisseurs, le gouvernement, les systèmes publics, etc.

Pour rester compétitives, la plupart de ces fournisseurs et sous-traitants auront (et devraient avoir) la capacité d'anticiper, de s'adapter et d'improviser pendant et après une perturbation.

Par conséquent, la résilience de toute organisation ou entreprise est le résultat ou dépend de l'interaction du système mis à l'épreuve avec les autres pendant la perturbation. Chaque organisation ou entreprise est à la fois résiliente et vulnérable,

all interconnected, interdependent organizations. Any business or organization tested in a silo will yield inaccurate or delusional test results and is likely to be the cause of delays/failure during an actual disruption.

The Covid -19 pandemic showed us exactly that. Many organizations, which claimed to conduct regular BCP testing for pandemic scenarios, suddenly discovered weak points, especially where plans depended on local government orders and complex policies that had never been anticipated or given proper attention.

For example, in India and the Philippines, it was clear that people would have to work from home during lockdowns. However, allowing employees to take devices outside the office required certain government permissions. This extra step caused long wait-times and unexpected operational delays.

Similarly, demand for laptops and home offce equipment skyrocketed, and vendors were scrambling to meet critical requirements. Organizations with weak contracts or single-vendor dependencies paid a heavy price for delays and business impacts.

Thus, the resilience of your business/ organization is also directly dependent on the resilience of your business partners or vendors; in other words, it is as strong as your weakest partner or supplier.

Well, this is mostly acknowledged by mature organizations. However, the trouble doesn't end here. In fact, it could be widely misleading to get comfortable with merely identifying the suppliers/ vendors you are dependent on. It's the vendors that you would have ignored or tagged as non-critical that you should be worried about. The weakest link is rarely the worst vendor, but usually the one that is assumed to be fine.

selon l'état des autres organisations, systèmes ou fournisseurs avec lesquels elle interagit.

La résilience est le processus qui mettra à l'épreuve les stratégies de continuité de toutes les organisations interconnectées et interdépendantes. Toute entreprise ou organisation testée de manière isolée donnera des résultats inexacts ou trompeurs et sera susceptible d'être à l'origine de retards ou d'échecs lors d'une perturbation réelle.

La pandémie de Covid-19 nous l'a clairement démontré. De nombreuses organisations, qui affirmaient mener régulièrement des tests de PCA pour des scénarios de pandémie, ont soudainement découvert des points faibles, en particulier lorsque les plans dépendaient d'ordonnances des autorités locales et de politiques complexes qui n'avaient jamais été anticipées ou prises en compte de manière adéquate.

Par exemple, en Inde et aux Philippines, il était clair que les gens devraient travailler à domicile pendant le confinement. Cependant, pour permettre aux employés d'emporter leurs appareils en dehors du bureau, certaines autorisations gouvernementales étaient nécessaires. Cette étape supplémentaire a entraîné de longs délais d'attente et des retards opérationnels imprévus.

De même, la demande d'ordinateurs portables et d'équipements de bureau à domicile a explosé, et les fournisseurs se sont efforcés de répondre aux besoins critiques. Les organisations dont les contrats étaient peu solides ou qui dépendaient d'un seul fournisseur ont payé le prix fort pour les retards et les répercussions sur leurs activités.

Ainsi, la résilience de votre entreprise/ organisation dépend également directement de la résilience de vos partenaires commerciaux ou fournisseurs ; en d'autres termes, elle est aussi forte que votre partenaire ou fournisseur le plus faible.

Ceci est généralement reconnu par les organisations matures. Cependant, le problème ne s'arrête pas là. En fait, il pourrait être très

Let us discuss some uncomfortable realities of Third-party/Supply chain Resilience.

What most organizations do is tick in the box controls, like:

1. Tiering of suppliers
2. Applying a risk-based approach to assess them
3. Reporting and reassuring based on the above approach

What is missing in a traditional Supply-chain/ third-party risk management:

1. Visibility or assessment of the noncritical vendors below the Tier-1 category.
2. It remains a trust-based optimism or a low-level assessment.
3. Periodic review of the categorization methodology of the vendors. There could be vendors who would have started to serve a critical function, or maybe a critical function has an indirect dependency on a non-critical vendor.

« GESTION DES FOURNISSEURS »

trompeur de se contenter d'identifier les fournisseurs dont vous dépendez. Ce sont les fournisseurs que vous auriez ignorés ou considérés comme non essentiels qui devraient vous préoccuper. Le maillon faible est rarement le pire fournisseur, mais généralement celui que l'on suppose être fiable.

Examinons quelques réalités dérangeantes concernant la résilience des tiers/de la chaîne d'approvisionnement.

La plupart des organisations se contentent de cocher des cases, par exemple :

1. Classification des fournisseurs
2. Application d'une approche basée sur les risques pour les évaluer
3. Rapports et assurances basés sur l'approche ci-dessus

Ce qui manque dans la gestion traditionnelle des risques liés à la chaîne d'approvisionnement/aux tiers :

1. La visibilité ou l'évaluation des fournisseurs non critiques en dessous de la catégorie Tier-1.
2. Il s'agit toujours d'un optimisme fondé sur la confiance ou d'une évaluation de bas niveau.
3. Révision périodique de la méthodologie de catégorisation des fournisseurs. Il peut y avoir des fournisseurs qui ont commencé à remplir une fonction critique, ou peut-être qu'une fonction critique dépend indirectement d'un fournisseur non critique. Il peut s'agir de fournisseurs profondément intégrés dans les flux de travail (centres d'appels, achats, paie, assistance juridique, etc.).
4. Un fournisseur, une région, une plateforme. Il s'agit d'un risque de concentration déguisé en modèle efficace, principalement conseillé par l'équipe financière. C'est le maillon faible dont dépend votre organisation.
5. Aucune visibilité sur les fournisseurs de quatrième niveau. Oui, ceux avec lesquels nous n'avons pas de contrat direct, mais qui sont des sous-traitants de votre fournisseur. Le fournisseur ne vous rend

These could be the vendors that are deeply embedded in the workflows (call centers, procurements, payroll, legal support, etc.).

4. One vendor, one region, one platform. This is a concentration risk disguised as an efficient model, mostly advised by the finance team. This is the one weak link your organization depends on.
5. No visibility on the fourth-party vendors. Yes, the ones that we don't have a direct contract with but are sub-vendors of your vendor. The supplier doesn't report to you, but their failure will eventually hurt the business.

If the Business Continuity Plan fails to map these dependencies, the plan is at risk. When such vendors fail, everything else fails simultaneously.

What Resilient Organizations do right:

1. Impact -based approach instead of focusing on vendors with big brands, the focus is on which is the critical activity and what can disrupt it. Then work backwards in mapping the dependencies and plan for making it resilient. For e.g Big retailers usually focus on resilience of major logistics partners, warehouses, and national carriers. But a large Toronto-based chain discovered a very different weak link – A transportation brokerage firm that coordinated last -mile deliveries between warehouses and stores. This small vendor went offline due to a cyber incident. As a result, trucks weren't routed, store replenishment stalled and perishable goods were wasted. One small routing broker was the single point of failure. Weak link: a "low risk" Tier-3 vendor controlling the data pipe between carriers and stores.
2. Build redundancies. Multiple suppliers for the same service cost more but prevent an existential crisis. Redundancy is the insurance, and not inefficiency. A decent cost-benefit analysis will help to convince the finance department.

pas compte, mais sa défaillance finira par nuire à l'entreprise.

Si le plan de continuité des activités ne parvient pas à cartographier ces dépendances, le plan est compromis. Lorsque ces fournisseurs échouent, tout le reste échoue simultanément.

Ce que font les organisations résilientes :

1. Approche axée sur l'impact : plutôt que de se concentrer sur les fournisseurs de grandes marques, l'accent est mis sur les activités critiques et les facteurs susceptibles de les perturber. Il s'agit ensuite de remonter la chaîne pour cartographier les dépendances et planifier la mise en place d'une résilience. Par exemple, les grands détaillants se concentrent généralement sur la résilience des principaux partenaires logistiques, des entrepôts et des transporteurs nationaux. Mais une grande chaîne basée à Toronto a découvert un maillon faible très différent : une société de courtage en transport qui coordonnait les livraisons du dernier kilomètre entre les entrepôts et les magasins. Ce petit fournisseur a cessé ses activités en raison d'un incident cybernétique. En conséquence, les camions n'ont pas pu être acheminés, le réapprovisionnement des magasins a été interrompu et les denrées périssables ont été gaspillées. Un petit courtier en acheminement était le seul point de défaillance. Maillon faible : un fournisseur de niveau 3 « à faible risque » contrôlant le flux de données entre les transporteurs et les magasins.
2. Mettre en place des redondances. Avoir plusieurs fournisseurs pour le même service coûte plus cher, mais permet d'éviter une crise existentielle. La redondance est une assurance, et non une source d'inefficacité. Une analyse coûts-avantages correcte aidera à convaincre le service financier.
3. Soumettez tous ces systèmes et fournisseurs interconnectés à des tests de résistance, comme vous le feriez pour vos propres plans. Fixez des objectifs de maturité pour tous les tests et exercices dans le but d'identifier les lacunes, les angles morts de l' et les maillons faibles. Testez les réponses à des scénarios réels, tels que les pannes

3. Stress testing all those interconnected systems and vendors , just like testing your own plans. Assign maturity targets for all the tests and exercises with an objective to identify gaps, blind spots, and weak links. Test responses to real-life scenarios, like cloud outages, vendor insolvency, geopolitical disruptions, cyberattacks on vendors' systems, etc. Most supply chain failures are not sudden or unexpected but due to expected dependencies that were never tested seriously.
4. Treat vendor failures as learning events . Instill confidence in the vendor to report even small events. Learnings should mean a review/update of:
   a. dependency mapping,
   b. contract
   c. exit strategy
   d. design assumptions, etc.

If nothing changes after a disruption, we are asking for a repeat of the same disruption. Faith in our ability to survive any disruption can make us complacent about the need for structural change.

For Organizational Resilience, a little cross-system and cross-vendor pessimism will go a long way in preventing potential threats. Sitting on an island as an optimistic business is not an option. Ω

ABOUT THE AUTHOR

Seema Verma *(CBCP, BCCE, LA ISO 22301, ISO 27001) is the Co-Founder and CEO of Medilinks Canada, a newly founded healthcare Start-Up. She has previously headed Business Continuity & Resiliency for Accenture Operations India, managing the enterprise-wide resilience program. She has driven major Continuity, ITDR, vendor risk, and crisis-management programs across APAC & NA for more than 20 years, in various capacities of Risk & Resilience roles at Deutsche Bank, RBS, and ABN AMRO. Her early career as a Lieutenant Commander in the Indian Navy shaped her expertise in large-scale Supply chain management, Disaster management, and Operational Logistics. Across three decades, she has built a reputation as a strategic, crisis-tested leader in Resilience, Governance, and Enterprise Risk.*

de cloud, l'insolvabilité des fournisseurs, les perturbations géopolitiques, les cyberattaques sur les systèmes des fournisseurs, etc. La plupart des défaillances de la chaîne d'approvisionnement ne sont pas soudaines ou inattendues, mais dues à des dépendances prévisibles qui n'ont jamais été testées sérieusement.
4. Considérez les défaillances des fournisseurs comme des occasions d'apprendre . Incitez les fournisseurs à signaler même les événements mineurs. Les enseignements tirés doivent se traduire par une révision/mise à jour des éléments suivants :
   a. cartographie des dépendances,
   b. du contrat
   c. stratégie de sortie
   d. hypothèses de conception, etc.

Si rien ne change après une perturbation, nous nous exposons à une répétition de cette même perturbation. La confiance en notre capacité à survivre à toute perturbation peut nous rendre complaisants quant à la nécessité d'un changement structurel.

Pour la résilience organisationnelle, un peu de pessimisme intersystémique et interfournisseurs contribuera grandement à prévenir les menaces potentielles. Il n'est pas envisageable de rester isolé en tant qu'entreprise optimiste. Ω

À PROPOS DE L'AUTEUR

Seema Verma *(CBCP, BCCE, LA ISO 22301, ISO 27001) est cofondatrice et PDG de Medilinks Canada, une start-up nouvellement créée dans le domaine des soins de santé. Elle a précédemment dirigé le département Continuité des activités et résilience chez Accenture Operations India, où elle gérait le programme de résilience à l'échelle de l'entreprise. Elle a dirigé d'importants programmes de continuité, d'ITDR, de gestion des risques liés aux fournisseurs et de gestion de crise dans les régions APAC et NA pendant plus de 20 ans, occupant divers postes dans le domaine des risques et de la résilience chez Deutsche Bank, RBS et ABN AMRO. Ses débuts de carrière en tant que capitaine de corvette dans la marine indienne lui ont permis d'acquérir une expertise dans la gestion de la chaîne d'approvisionnement à grande échelle, la gestion des catastrophes et la logistique opérationnelle. Au cours des trois dernières décennies, elle s'est forgé une réputation de leader stratégique et aguerri en matière de résilience, de gouvernance et de risques d'entreprise.*

TRUE NORTH RESILIENCE
Résilience du vrai nord
DRI Canada's magazine / Magazine de DRI Canada

Call for Articles

Submissions are welcome where they share best practices, experiences, and opinions that are fact-based, non-partisan, and have been generated without the use of Artificial Intelligence tools. We do not accept articles that promote specific businesses, or products, unless it's intrinsic to the narrative of the article. We are pleased to use this publication to share ideas that will serve professional development and thought leadership through continual improvement in Resilience.

Please make all editorial submissions to editors@dri.ca.

Submission Guidelines

Suggested topics:
- Resilience, Cyber Security, Data Protection, Privacy, Business Continuity, Disaster Recovery, Crisis Management, Emergency Management, OH&S, Risk Management

Word count:
- Preferably 500-2,000 words (maximum 2,500)

Vendor-neutral:
- No mention of any for profit organization product, or service will be published in the magazine (except for paid advertisements).

Copyright:
- Every magazine article published will be copyrighted by DRI Canada.
- Authors are required to sign a copyright agreement.
- Articles must be original and may not be simultaneously submitted to other publications.
- DRI Canada will retain all publishing rights. However, permission will be granted for marketing purposes or any other non-competing publication with attribution.

Required materials: All article submissions must include a short biography and a headshot photo of the author.

Art: Photographs or graphic elements may accompany each article. Graphic submissions are welcome but please refrain from designing your article submission.
- Please submit text and graphic elements separately.
- Photos and graphics must be high resolution (300 dpi at 100% print size) or vector based.

Authors: Articles from DRI Certified Professionals are given preference. Not applicable to student submissions.

Editing: Articles will be edited for length, clarity, style, and improper usage of industry terms. Ω

Appel à articles

Les soumissions sont les bienvenues lorsqu'elles partagent des bonnes pratiques, des expériences et des opinions fondées sur des faits, non partisanes et générées sans l'utilisation d'outils d'intelligence artificielle. Nous n'acceptons pas les articles qui font la promotion d'entreprises ou de produits spécifiques, à moins que cela ne soit intrinsèque à la narration de l'article. Nous sommes heureux d'utiliser cette publication pour partager des idées qui serviront au développement professionnel et au leadership éclairé par l'amélioration continue de la résilience.

Veuillez adresser vos propositions éditoriales à editors@dri.ca.

Lignes directrices pour les soumissions

Sujets proposés :
- Résilience, cybersécurité, protection des données, Protection de la vie privée, Continuité des activités, Reprise après sinistre, Gestion de crise, Gestion des urgences, Santé et sécurité au travail, Gestion des risques

Nombre de mots :
- De préférence entre 500 et 2 000 mots (maximum 2 500)

Neutralité vis-à-vis des fournisseurs :
- Aucune mention d'un produit ou d'un service d'une organisation à but lucratif ne sera publiée dans le magazine (à l'exception des publicités payantes).

Droits d'auteur :
- Chaque article publié dans le magazine sera protégé par les droits d'auteur de DRI Canada.
- Les auteurs sont tenus de signer un accord sur les droits d'auteur.
- Les articles doivent être originaux et ne peuvent être soumis simultanément à d'autres publications.
- DRI Canada conservera tous les droits de publication. Cependant, une permission sera accordée à des fins de marketing ou pour toute autre publication non concurrente, avec mention de la source.

Matériel requis : Toutes les soumissions d'articles doivent inclure une courte biographie et une photo de l'auteur.

Art : Des photographies ou des éléments graphiques peuvent accompagner chaque article. Les propositions graphiques sont les bienvenues, mais nous vous demandons de ne pas concevoir votre article.
- Veuillez soumettre le texte et les éléments graphiques séparément
- Les photos et les graphiques doivent être en haute résolution (300 dpi à 100 % de la taille d'impression) ou vectoriels.

Auteurs : Les articles rédigés par des professionnels certifiés par DRI sont privilégiés. Cette règle ne s'applique pas aux articles soumis par des étudiants.

Révision : Les articles seront édités pour des raisons de longueur, de clarté, de style et d'utilisation incorrecte des termes de l'industrie. Ω

Enterprise Resilience is More Than BCM 2.0

La résilience d'entreprise va au-delà du BCM 2.0

By/Par **Matthew Schwarz**

Abstract:
In an era of systemic and prolonged disruptions, ranging from cyberattacks and supply chain failures to regulatory shifts and extreme weather, traditional Business Continuity Management (BCM) is no longer sufficient. Designed for short-lived crises, BCM struggles to address today's complex, interconnected, chronic risks.

This article introduces the approach one organization adopted for Enterprise Resilience (ER) as a strategic, multi-dimensional capability that goes beyond BCM's recovery focus to embed resilience across organizational priorities. ER integrates governance, capability maturity, and cross-functional coordination through a Centre of Expertise model, leveraging existing structures for lean and economical operation. ER encompasses cyber resilience, IT disaster recovery, third-party risk management, and cultural adaptability,

Résumé :
À une époque marquée par des perturbations systémiques et prolongées, allant des cyberattaques et des défaillances de la chaîne d›approvisionnement aux changements réglementaires et aux conditions météorologiques extrêmes, la gestion traditionnelle de la continuité des activités (BCM) n›est plus suffisante. Conçue pour des crises de courte durée, la BCM peine à faire face aux risques complexes, interconnectés et chroniques d›aujourd›hui.

Cet article présente l'approche adoptée par une organisation en matière de résilience d'entreprise (ER) en tant que capacité stratégique et multidimensionnelle qui va au-delà de l'objectif de reprise du BCM pour intégrer la résilience dans toutes les priorités organisationnelles. L'ER intègre la gouvernance, la maturité des capacités et la coordination interfonctionnelle grâce à un modèle de centre d'expertise, en tirant parti des structures existantes pour un fonctionnement rationnel et économique. L'ER englobe la

ensuring organizations can prevent, absorb, and adapt to disruptions rather than merely recover.

By aligning resilience with enterprise strategy, mapping interdependencies, and institutionalizing continuous improvement, this approach transforms resilience from a compliance exercise into a competitive advantage. Enterprise Resilience is not BCM 2.0, it is a shift enabling organizations to thrive amid volatility.

In today's world, organizations face a growing array of threats; cyberattacks, supply chain disruptions, regulatory shifts, extreme weather, and geopolitical instability. Traditional Business Continuity Management (BCM), while foundational, is increasingly insufficient to address the complexity, and speed of modern disruptions; they are both systemic and systematic! BCM after all, was designed for the recovery from an acute crisis – quick, painful, and then gone. Disruptions today are neither quick nor gone, and too often we're left with the pain.

To ameliorate this, the idea of Enterprise Resilience (ER) has emerged to reinforce organizations' ability to respond by expanding where BCM was limited. It is, however, not merely an evolution, what some might call

cyber-résilience, la reprise après sinistre informatique, la gestion des risques liés aux tiers et l'adaptabilité culturelle, garantissant ainsi que les organisations peuvent prévenir, absorber et s'adapter aux perturbations plutôt que de se contenter de se rétablir.

En alignant la résilience sur la stratégie d'entreprise, en cartographiant les interdépendances et en institutionnalisant l'amélioration continue, cette approche transforme la résilience d'un exercice de conformité en un avantage concurrentiel. La résilience d'entreprise n'est pas une version 2.0 de la BCM, c'est un changement qui permet aux organisations de prospérer dans un contexte de volatilité.

Dans le monde actuel, les organisations sont confrontées à un éventail croissant de menaces : cyberattaques, perturbations de la chaîne d'approvisionnement, changements réglementaires, conditions météorologiques extrêmes et instabilité géopolitique. La gestion traditionnelle de la continuité des activités (BCM), bien que fondamentale, est de plus en plus insuffisante pour faire face à la complexité et à la rapidité des perturbations modernes, qui sont à la fois systémiques et systématiques ! Après tout, la BCM a été conçue pour permettre de se remettre d'une crise aiguë, rapide, douloureuse, puis passagère. Aujourd'hui, les perturbations ne sont ni rapides ni passagères, et trop souvent, nous en subissons les conséquences.

Pour remédier à cela, le concept de résilience d'entreprise (ER) a vu le jour afin de renforcer la capacité des organisations à réagir en élargissant les limites de la BCM. Il ne s'agit toutefois pas simplement d'une évolution, que certains pourraient appeler « BCM 2.0 », mais d'une approche fondamentalement plus large et plus intégrée. La résilience d'entreprise englobe non seulement la planification de la continuité des processus, mais aussi la cyber-résilience, la robustesse de l'infrastructure informatique, la gestion des risques liés aux tiers et la culture organisationnelle, c'est-à-dire tous les types de menaces mentionnés ci-dessus et bien d'autres encore. Il s'agit de garantir que les perturbations, quelle que soit leur gravité ou leur durée, ne causent pas de dommages intolérables à l'entreprise.

"BCM 2.0", but a fundamentally broader and more integrated approach. Enterprise Resilience encompasses not only continuity planning around processes, but also cyber resilience, IT infrastructure robustness, third-party risk management, and organizational culture – all those threat types and more, mentioned above. It is about ensuring that disruptions, no matter how severe or prolonged, do not cause intolerable harm to the enterprise.

Resilient organizations have embraced this shift through its Enterprise Resilience program, which integrates governance, capability maturity, and cross-functional coordination into a unified framework. This article explores three key aspects that distinguish Enterprise Resilience from traditional BCM: its strategic integration with enterprise priorities, its multi-dimensional scope, and its emphasis on governance and continuous maturity. Together, these elements demonstrate why Enterprise Resilience is not just a rebranded continuity plan, but something that brings together expertise to build a stronger organization.

One of the most significant distinctions between Enterprise Resilience and traditional BCM lies in its strategic integration. While BCM typically operates as a function focused on process-recovery planning, Enterprise Resilience is embedded within the broader enterprise strategy by incorporating corporate growth priorities, aligning resilience efforts across functions, bringing risk appetite into the operations of the business, leading to long-term value protection by identifying and reinforcing the organization's critical functions.

At all organizations, programs begins with a comprehensive inventory and maturity assessment of existing capabilities, providing a data-driven foundation for prioritizing the investment of time. These include risk taxonomies, process taxonomies, risk registers, and subject-matter interviews. It is important to emphasize this data-inventory point – even immature organizations have data on risk events that have materialized

Les organisations résilientes ont adopté cette évolution grâce à leur programme de résilience d'entreprise, qui intègre la gouvernance, la maturité des capacités et la coordination interfonctionnelle dans un cadre unifié. Cet article explore trois aspects clés qui distinguent la résilience d'entreprise du BCM traditionnel : son intégration stratégique aux priorités de l'entreprise, sa portée multidimensionnelle et l'accent mis sur la gouvernance et la maturité continue. Ensemble, ces éléments démontrent pourquoi la résilience d'entreprise n'est pas simplement un plan de continuité rebaptisé, mais quelque chose qui rassemble l'expertise nécessaire pour bâtir une organisation plus forte.

L'une des distinctions les plus significatives entre la résilience d'entreprise et la gestion traditionnelle de la continuité des activités réside dans son intégration stratégique. Alors que la gestion de la continuité des activités fonctionne généralement comme une fonction axée sur la planification de la reprise des processus, la résilience d'entreprise s'inscrit dans la stratégie globale de l'entreprise en intégrant les priorités de croissance de l' , en alignant les efforts de résilience entre les fonctions, en intégrant l'appétit pour le risque dans les opérations de l'entreprise, ce qui conduit à une protection de la valeur à long terme en identifiant et en renforçant les fonctions critiques de l'organisation.

Dans toutes les organisations, les programmes commencent par un inventaire complet et une évaluation de la maturité des capacités existantes, fournissant ainsi une base fondée sur des données pour hiérarchiser les investissements en temps. Cela comprend les taxonomies des risques, les taxonomies des processus, les registres des risques et les entretiens avec des experts en la matière. Il est important de souligner cet aspect de l'inventaire des données : même les organisations immatures disposent de données sur les événements à risque qui se sont matérialisés dans le passé. Elles peuvent ou non être suivies dans les rapports sur les pertes et les registres des risques, mais elles le seront certainement grâce à la sagesse accumulée des employés chevronnés. L'utilisation de ces sources de données garantit que les initiatives de résilience sont

in the past. They may or not be tracked on loss reporting and risk registers but certainly will be through accumulated wisdom of seasoned employees. Using these sources of data ensures that resilience initiatives are defendable and forward-looking, targeting the most critical gaps (and we know they're gaps – a risk has crystallized into an issue!) while aligning with business objectives – and can be applied regardless of organizational size.

Governance, another pillar, plays a central role in this integration. As risk professionals, it's our responsibility to ensure that our programs operate in lean and economical fashions; we're value-protectors, not revenue-drivers. To that end, and to ensure true multi-dimensionality, the resilient organization adopted a **Centre of Expertise** (CoE) model for Enterprise Resilience. This acts as a strategic enabler, coordinating across business units and risk pillars to ensure consistency, accountability, and executive visibility.

At the resilient organization, the CoE is responsible for defining the Target Operating Model, establishing impact tolerances, and the strategic integration by embedding resilience into existing governance documents, existing activities, and existing enterprise priorities. This is a key point to operating economically - the CoE is not about building something new. It is about leveraging existing expertise, reporting lines, and functions to move resilience activities forward together. And here's an important aside: almost all organizations already have the foundations of this expertise. There will be a supplier team (or person), an HR team (or person), and a technical team (or person – sigh). As your organization grows, these functions mature and expand and specialize, but will be there from, well not day one, but maybe day 3 or 4. A CoE can fit into almost any organization because it is designed to fit in, not be added on.

Enterprise Resilience is a multi-dimensional capability that integrates resilience across domains: BCM, IT, cyber, operational, and human. This comprehensive approach ensures

défendables et tournées vers l'avenir, ciblant les lacunes les plus critiques (et nous savons qu'il s'agit de lacunes, car un risque s'est cristallisé en un problème !) tout en s'alignant sur les objectifs commerciaux, et peuvent être appliquées quelle que soit la taille de l'organisation.

La gouvernance, autre pilier, joue un rôle central dans cette intégration. En tant que professionnels du risque, il est de notre responsabilité de veiller à ce que nos programmes fonctionnent de manière rationnelle et économique ; nous sommes des protecteurs de valeur, pas des générateurs de revenus. À cette fin, et afin de garantir une véritable multidimensionnalité, l'organisation résiliente a adopté un modèle de **centre d'expertise** (CoE) pour la résilience d'entreprise. Celui-ci agit comme un catalyseur stratégique, coordonnant les différentes unités commerciales et les piliers de risque afin de garantir la cohérence, la responsabilité et la visibilité de la direction.

Dans l'organisation résiliente, le CoE est chargé de définir le modèle opérationnel cible, d'établir les tolérances d'impact et l'intégration stratégique en intégrant la résilience dans les documents de gouvernance existants, les activités existantes et les priorités existantes de l'entreprise. C'est un point essentiel pour fonctionner de manière économique : le CoE ne vise pas à créer quelque chose de nouveau. Il s'agit de tirer parti de l'expertise, des lignes hiérarchiques et des fonctions existantes pour faire avancer ensemble les activités de résilience. Et voici une remarque importante : presque toutes les organisations disposent déjà des bases de cette expertise. Il y aura une équipe (ou une personne) chargée des fournisseurs, une équipe (ou une personne) chargée des ressources humaines et une équipe (ou une personne – soupir) chargée des aspects techniques. Au fur et à mesure que votre organisation se développe, ces fonctions mûrissent, se développent et se spécialisent, mais elles seront présentes dès le troisième ou quatrième jour, et non dès le premier. Un CoE peut s'intégrer dans presque toutes les organisations, car il est conçu pour s'adapter et non pour être ajouté.

that the organization is not only prepared to respond to disruptions but is also equipped to prevent, absorb, and adapt with them. For example, the resilient organization's program includes dedicated streams for Cyber Resiliency, Disaster Recovery, Third-Party Risk Management, Business Continuity Management, and Human Resilience & Culture, each with its own governance, maturity goals, and integration points. Enterprise Resilience's multi dimensional scope gives it a unique opportunity to support those streams integration with the organization's strategic priorities.

This strategic integration transforms the day-to-day tasks from a compliance-driven activity into a value-protecting capability. By integrating resilience into existing operations, investments, and governance processes, the organization ensures that its ability to withstand disruption is not an afterthought, but a competitive advantage. And is done in a lean and economical way. This is not compliance-as-governance, but governance based on its root – to govern.

La résilience d'entreprise est une capacité multidimensionnelle qui intègre la résilience dans tous les domaines : BCM, informatique, cyber, opérationnel et humain. Cette approche globale garantit que l'organisation est non seulement prête à réagir aux perturbations, mais également équipée pour les prévenir, les absorber et s'y adapter. Par exemple, le programme d'une organisation résiliente comprend des volets dédiés à la cyber-résilience, à la reprise après sinistre, à la gestion des risques liés aux tiers, à la gestion de la continuité des activités et à la résilience humaine et la culture, chacun avec sa propre gouvernance, ses propres objectifs de maturité et ses propres points d'intégration. La portée multidimensionnelle de la résilience d'entreprise lui confère une opportunité unique de soutenir l'intégration de ces volets avec les priorités stratégiques de l'organisation.

Cette intégration stratégique transforme les tâches quotidiennes d'une activité axée sur la conformité en une capacité de protection de la valeur. En intégrant la résilience dans les opérations, les investissements et

Enterprise Resilience also addresses the growing importance of third-party risk and data governance within the Canadian regulatory framework – remember regulatory shifts are a disruption type as material as any other. The organisation's Third-Party Risk Management (TPRM) framework aligns with regulatory guidelines, ensuring that resilience is embedded throughout the lifecycle of vendor relationships, from onboarding and classification to ongoing due diligence and offboarding. Similarly, the data governance function plays a critical role in maintaining data integrity and access governance. Enterprise Resilience supports these risk management streams as they integrate themselves with cyber resilience, ITDR, and BCM, which directly leads to a more resilient organization.

For a practical example at the resilient organization: BCM will identify critical processes and their dependencies – both IT and third party. Information Technology Disaster Recovery (ITDR) and cyber resilience will ensure the third-party vendors can support their confidentiality, integrity, and

les processus de gouvernance existants, l'organisation s'assure que sa capacité à résister aux perturbations n'est pas une réflexion après coup, mais un avantage concurrentiel. Et cela se fait de manière rationnelle et économique. Il ne s'agit pas de conformité en tant que gouvernance, mais de gouvernance basée sur sa racine : gouverner.

La résilience d'entreprise tient également compte de l'importance croissante des risques liés aux tiers et de la gouvernance des données dans le cadre réglementaire canadien. N'oubliez pas que les changements réglementaires sont un type de perturbation aussi important que les autres. Le cadre de gestion des risques liés aux tiers (TPRM) de l'organisation s'aligne sur les directives réglementaires, garantissant que la résilience est intégrée tout au long du cycle de vie des relations avec les fournisseurs, de l'intégration et la classification à la diligence raisonnable continue et au départ. De même, la fonction de gouvernance des données joue un rôle essentiel dans le maintien de l'intégrité des données et la gouvernance de l'accès. La résilience d'entreprise soutient ces flux de gestion des risques, car ils s'intègrent à la cyber-résilience, à l'ITDR et au BCM, ce qui conduit directement à une organisation plus résiliente.

Voici un exemple pratique dans une organisation résiliente : le BCM identifie les processus critiques et leurs dépendances, tant au niveau informatique que tiers. La reprise après sinistre informatique (ITDR) et la cyber-résilience garantissent que les fournisseurs tiers peuvent respecter leurs engagements en matière de confidentialité, d'intégrité et de disponibilité, tandis que le TPRM facilite l'évaluation des risques liés aux fournisseurs, notamment en soutenant les discussions sur la planification d'urgence en cas de perte de fournisseurs. La résilience d'entreprise rassemble ces flux de manière holistique, plutôt que de les traiter de manière ponctuelle dans le cadre de projets ou d'intégrations spécifiques. Quelle que soit la taille de votre organisation, le fait de faire dialoguer les experts de ces flux, puis de les faire travailler ensemble, fait considérablement progresser la résilience.

availability commitments, and TPRM facilitates vendor risk assessments, including supporting conversations on vendor-loss contingency planning. Enterprise Resilience brings these streams together in a holistic way, instead of one-off engagements around specific projects or onboardings. Regardless of the size of your organization, getting the experts from these streams talking to each other, and then working with each other, materially moves the needle on resilience.

Finally, Enterprise Resilience emphasizes the mapping of interdependencies across services and systems; similar to Swiss-cheese, risks materialize where they slip through gaps in risk-management controls. You need to be able to see the mapping to understand where gaps are if you want to be proactive in your prevention efforts. The resilient organization's approach includes tiering business services and identifying critical processes and then mapping internal service dependencies. This enables a more accurate understanding of systemic risk and ensures that resilience efforts are targeted where they matter most going back to that important consideration: value-protectors must be lean and economical in their operation and allow decision makers to be lean and economical in where they allocate time and money.

As a closing point, and it'll come as no surprise to risk professionals, but Enterprise Resilience is not a static plan, it is a dynamic capability that evolves through structured governance, continuous assessment, and iterative improvement. This distinguishes it sharply from traditional BCM, which often relies on periodic plan updates and isolated testing exercises, despite all our best efforts at building a "continuous BIA".

Enterprise Resilience is not simply an upgraded version of Business Continuity Management, it is a fundamentally different paradigm. Where BCM focuses on recovery, Enterprise Resilience emphasizes readiness. Where BCM is often operationally siloed, Enterprise Resilience is strategically integrated. And where BCM tends to be static, Enterprise

Enfin, la résilience d'entreprise met l'accent sur la cartographie des interdépendances entre les services et les systèmes ; à l'instar du fromage suisse, les risques se matérialisent là où ils passent à travers les mailles du filet des contrôles de gestion des risques. Vous devez être en mesure de visualiser cette cartographie pour comprendre où se trouvent les lacunes si vous souhaitez être proactif dans vos efforts de prévention. L'approche d'une organisation résiliente consiste à hiérarchiser les services commerciaux, à identifier les processus critiques, puis à cartographier les dépendances internes entre les services. Cela permet de mieux comprendre les risques systémiques et de s'assurer que les efforts de résilience sont ciblés là où ils sont le plus importants, ce qui nous ramène à cette considération essentielle : les protecteurs de valeur doivent être efficaces et économiques dans leur fonctionnement et permettre aux décideurs d'être efficaces et économiques dans l'allocation de leur temps et de leur argent.

Pour conclure, et cela ne surprendra pas les professionnels du risque, la résilience d'entreprise n'est pas un plan statique, mais une capacité dynamique qui évolue grâce à une gouvernance structurée, une évaluation continue et une amélioration itérative. Cela la distingue nettement de la gestion traditionnelle de la continuité des activités (GCA), qui repose souvent sur des mises à jour périodiques des plans et des exercices de test isolés, malgré tous nos efforts pour mettre en place une « analyse d›impact sur les activités (AIA) continue ».

La résilience d'entreprise n'est pas simplement une version améliorée de la gestion de la continuité des activités, c'est un paradigme fondamentalement différent. Alors que la gestion de la continuité des activités se concentre sur la reprise, la résilience d'entreprise met l'accent sur la préparation. Alors que la gestion de la continuité des activités est souvent cloisonnée sur le plan opérationnel, la résilience d'entreprise est intégrée de manière stratégique. Et alors que la gestion de la continuité des activités a tendance à être statique, la résilience d'entreprise est dynamique, évoluant

Resilience is dynamic, continuously evolving through governance, through talking, and through testing. The goal is not to return to business-as-usual once the disruption is over, but to absorb and adapt to significant changes in the environment.

The resilient organization's Enterprise Resilience program exemplifies this shift. By aligning resilience with enterprise strategy, embedding it across multiple dimensions of risk, and institutionalizing governance and maturity assessments, the organization has built a capability that is both comprehensive and adaptive. The CoE, the integration of third-party and data governance, and the emphasis on impact tolerance and service tiering all reflect a forward-thinking approach that goes far beyond traditional continuity planning.

In an era where disruption is now a daily event, organizations must move beyond the confines of BCM. Enterprise Resilience offers a blueprint for doing so, one that enables organizations not just to survive disruption, but to emerge stronger from it. For resilience professionals, the imperative is clear: embrace Enterprise Resilience not as a rebranding exercise, but as a strategic transformation.

Disclaimer: This article was written in a personal capacity. The views and opinions expressed are solely those of the author and do not represent the views or positions of Export Development Canada (EDC) or its affiliates. Ω

continuellement grâce à la gouvernance, au dialogue et aux tests. L'objectif n'est pas de revenir au statu quo une fois la perturbation terminée, mais d'absorber les changements importants dans l'environnement et de s'y adapter.

Le programme de résilience d'entreprise d'une organisation résiliente illustre bien ce changement. En alignant la résilience sur la stratégie d'entreprise, en l'intégrant à plusieurs dimensions du risque et en institutionnalisant la gouvernance et les évaluations de maturité, l'organisation a développé une capacité à la fois complète et adaptative. Le CoE, l'intégration de la gouvernance des tiers et des données, et l'accent mis sur la tolérance aux impacts et la hiérarchisation des services reflètent tous une approche avant-gardiste qui va bien au-delà de la planification traditionnelle de la continuité.

À une époque où les perturbations sont désormais quotidiennes, les organisations doivent dépasser les limites de la gestion de la continuité des activités. La résilience d›entreprise offre un plan d›action pour y parvenir, qui permet aux organisations non seulement de survivre aux perturbations, mais aussi d›en sortir plus fortes. Pour les professionnels de la résilience, l›impératif est clair : adopter la résilience d›entreprise non pas comme un simple changement d›image, mais comme une transformation stratégique.

Avertissement : Cet article a été rédigé à titre personnel. Les points de vue et opinions exprimés sont ceux de l'auteur et ne reflètent pas les points de vue ou positions d'Exportation et développement Canada (EDC) ou de ses filiales. Ω

Matthew Schwarz is the Enterprise Resilience Lead at Export Development Canada. His work focuses on business continuity, crisis management, and organizational resilience, with an emphasis on translating complex risk frameworks into practical, decisionready capabilities. Outside of work he enjoys dodgeball, paddleboarding, and will be trying his hand at kite surfing.

Matthew Schwarz est responsable de la résilience des entreprises chez Exportation et développement Canada. Son travail porte principalement sur la continuité des activités, la gestion de crise et la résilience organisationnelle, avec un accent particulier sur la traduction de cadres de risque complexes en capacités pratiques et opérationnelles. En dehors du travail, il aime jouer au dodgeball, faire du paddleboard et s'essayer au kitesurf.

Notice:

The articles presented in ***True North Resilience*** reflect the viewpoints of their respective authors and do not necessarily represent the official stance of DRI Canada. Each author brings their unique perspective, shaped by their experiences and insights within the industry. The purpose of these articles is to foster respectful discourse and encourage critical examination of various aspects of our field.

We believe that promoting thought leadership and encouraging progressive thinking is essential for the growth and evolution of our industry. Readers are invited to interpret the content thoughtfully, considering diverse opinions and ideas. We encourage constructive dialogue, as it is through such discussions that we can enhance our understanding and drive positive change.

DRI Canada is committed to creating an inclusive environment where varying viewpoints can be shared and debated. However, we remind readers that the interpretations and conclusions drawn from these articles are the responsibility of the reader, and we encourage an open-minded approach to all discussions. Ω

Avis :

Les articles présentés dans ***True North Resilience*** reflètent les points de vue de leurs auteurs respectifs et ne représentent pas nécessairement la position officielle de DRI Canada. Chaque auteur apporte son point de vue unique, façonné par ses expériences et ses connaissances au sein de l'industrie. L'objectif de ces articles est de favoriser un discours respectueux et d'encourager l'examen critique des divers aspects de notre domaine.

Nous pensons que la promotion d'un leadership éclairé et l'encouragement d'une pensée progressiste sont essentiels à la croissance et à l'évolution de notre secteur. Les lecteurs sont invités à interpréter le contenu de manière réfléchie, en tenant compte des diverses opinions et idées. Nous encourageons un dialogue constructif, car c'est grâce à ces discussions que nous pouvons améliorer notre compréhension et susciter des changements positifs.

DRI Canada s'engage à créer un environnement inclusif où les différents points de vue peuvent être partagés et débattus. Cependant, nous rappelons aux lecteurs que les interprétations et les conclusions tirées de ces articles relèvent de leur responsabilité, et nous encourageons une approche ouverte à toutes les discussions. Ω

DRI CANADA

Train.
Prepare.
Recover.

DRI CANADA'S YEAR OF EXERCISE DESIGN

True North Resilience

ISSN 2816-900X

Return to TOC

Retour au sommaire