

## In this Issue:

- *BCP for Remote Workers*
- *Using a Framework*
- *Deliberate Design*
- *Cyberattacks*

and more...

## Dans ce numéro :

- *BCP pour les travailleurs à distance*
- *Utilisation d'un framework*
- *Conception délibérée*
- *Cyberattaques*

et plus encore...

**Inaugural Issue! | Numéro inaugural!**

**Congratulations to the editors of**  
***TRUE NORTH RESILIENCE***  
**and their inaugural issue!**

Continuity & Resilience Today and J&J Expositions are proud supporters and we look forward to many more issues

**Dan Joyce**  
President J&J Expos  
Event Director CRT

**April Joyce**  
Vice President J&J Expos  
Business Manager CRT

**NTINUITY & RESILIENCE TODAY**

INTERNATIONAL BUSINESS CONTINUITY MANAGEMENT CONFERENCE

[www.CRTDEMCON.ca](http://www.CRTDEMCON.ca)

# Contents | Le Sommaire

<b>President's Corner</b> .....	5	<b>Project Managing a Business Continuity and Disaster Recovery Program Build</b> .....	37
<b>Coin du président</b> <i>Brock Holowachuk, CBCP</i>		<b>Gestion de projet pour la construction d'un programme de continuité des activités et de reprise après sinistre</b> <i>Sukhmani Sandhu, PMP</i>	
<b>Editors' Desk</b> .....	6	<b>OUT WITH THE "OLD" AND IN WITH THE "NEW" Moving Beyond Business Continuity!</b> .....	39
<b>Bureau des redacteurs</b> <i>Garth Tucker, CBCP CORP</i>		<b>LE "VIEUX" S'EN VA ET LE "NOUVEAU" ARRIVE Aller au-delà de la continuité des activités!</b> <i>Reta Setrak, MBCP</i>	
<b>Encouraging Credibility and Professionalism</b> .....	7	<b>Business Continuity Planning for the Remote Worker</b> .....	42
<b>Encourager la crédibilité et le professionnalisme</b>		<b>Planification de la continuité des activités pour le travailleur à distance</b> <i>Vito Mangialardi, CBCP</i>	
<b>Cyberattacks: Stakeholder &amp; Responses</b> .....	8	<b>Leadership Highlight</b> .....	46
<b>La montée de la cybercriminalité</b> <i>Thibault Dambrine</i>		<b>Faits saillants du leadership</b> <i>Brock Holowachuck, CBCP</i>	
<b>Responding to a Disaster Using a Framework</b> .....	14	<b>Advertisers' Index</b> .....	47
<b>Intervention en cas de sinistre à l'aide d'un cadre</b> <i>Tim Lalonde</i>		<b>Index des annonceurs</b>	
<b>Advancing Table Top Exercise Development: Deliberate Design creates Remarkable Reports</b> .....	20		
<b>Faire progresser le développement d'exercices sur table : une conception délibérée crée des rapports remarquables</b> <i>Cynthia Wenn, MA CBCP CBCA CRM</i>			
<b>BCP in the Hybrid Working World</b> .....	33		
<b>BCP dans le monde du travail hybride</b> <i>Brenda Escribano, CBCP</i>			
<b>BIT Theory: Tracking Building Impacts during Business Continuity Incidents</b> .....	34		
<b>La théorie du BIT : Suivi des impacts sur les bâtiments pendant les incidents de continuité des activités</b> <i>Paul Swanburg, BAH</i>			



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](mailto:editors@dri.ca)  
Toll Free: 1-844-228-8135  
Local: 416-646-2750

©2022 Disaster Recovery Institute Canada. All rights reserved. Unless otherwise specified, all letters and articles received are assumed for publication and become the copyright property of True North Resilience if published.

©2022 Disaster Recovery Institute Canada. Tous droits réservés. Sauf indication contraire, toutes les lettres et tous les articles reçus sont supposés être publiés et deviennent la propriété de True North Resilience en cas de publication.

Send mailing list queries, and requests for reprints, bulk copies, or reprint permission by email to: [editors@dri.ca](mailto:editors@dri.ca), or by surface mail to: 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](mailto:editors@dri.ca), ou par courrier ordinaire à : 701 Rossland Road East, Suite 375, Whitby, ON, L1N 8Y9.

# TRUE NORTH RESILIENCE

MAGAZINE DE RÉSILIENCE DU VRAI NORD



## Board of Directors

### Conseil d'administration

The Board of Directors sets DRI CANADA's goals, strategic direction and policy, and offers guidance., under the guidelines and ethical direction set by DRI International. The Board is the 4 governing body of the DRI CANADA and is responsible for the business direction, policy making, public awareness and fiscal management of the organization.

**Brock Holowachuk**, CBCP  
President

**Nancy Holloway-White**, CBCP, CBCA  
Past President

**Lisa Maddock**, ABCP  
Secretary/Privacy Officer,  
Director Ontario Region

**Scott Leavitt**, CBCP  
Treasurer, Director Pacific Region

**Rejean Pesant**, CBCP  
Education Commission Chair and  
Director Quebec Region

**Rebecca Wade**, MBBCP  
Director Central Canada

**Devin McNaughton**, ABCP  
Director Western Region

**Jason Firlotte**, MBBCP, CBCV  
Director at Large

**Andrea Buchholz**, CBCLA  
Director at Large

**Brenda Escribano**, CBCP  
Director Atlantic Canada

**Garth Tucker**, CBCP, CORP  
Director Central Region

**Jeff Hortobagyi**, CBCP  
Director at Large

## Magazine Steering Committee

### Comité directeur du magazine

Executive Director **Perry Ruehlen**, CAE  
Editor-in-Chief **Garth Tucker**, CBCP, CORP  
Design Editor **Vaughn Dragland**, BA, ISP, PMP  
Associate Editor **Brock Holowachuk**, CBCP  
Associate Editor **Nancy Holloway-White**, CBCP, CBCA  
Associate Editor **Lisa Maddock**, ABCP  
Associate Editor **Réjean Pesant**, CBCP

## 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.

DRI Canada, and the DRI Canada logo are trademarks or registered trademarks of Disaster Recovery Institute Canada, in Canada and other countries.

Publishing and Graphic Design  
Eclipse Technologies Inc.  
C: 416-219-8790  
T: 416-622-8789  
[e-clipse.ca](http://e-clipse.ca)

Printing, Binding, and Lettershop  
Canmark Communications  
C: 416.553.8228  
T: 905.591.3354  
[canmarkcommunications.com](http://canmarkcommunications.com)



# President's Corner Coin du président

By/Par Brock Holowachuk  
President, DRI Canada



**W**e've learned a lot in the last two years. We've known for a long time that Continuity Management is an important element in the preparedness and safety of our nation. Covid not only proved that, but it also showed Canadians that the Certified Professionals of DRI Canada provide something important that makes our communities, business and organizations a safer place. It was a once-in-a-generation emergency, and the work we do has never been more important.

Likewise, the work of DRI Canada has never been more important. Advancing our profession isn't just important to our Certified Professionals ... the last two years have shown that it's important to all Canadians. We've seen that our work is really about public safety and security, and those needs are best met through a strong, not-for-profit that builds a community of Continuity Management professionals.

True North Resilience is about building that community. It's also about showing that our community is growing and evolving.

Our goal is to use this magazine to share information that not only shows the good work that's happening, but also looks to the future. Our work in Continuity Management has never been in isolation, and Covid showed that those connections are growing increasingly complex. You'll see that True North Resilience is designed to reflect the reality of our work, and draws in the perspective of the many partners that are shaping the work we do, and the direction of our profession.

I'd like to close with my thanks to the people who've been involved with making True North Resilience a

reality. Most importantly, I'd like to acknowledge the leadership and hard work of Garth Tucker from our Board of Directors. Garth saw the need, built the vision, and has led the work to make this happen. Thanks also to everyone who contributed an article. By sharing your experiences and perspectives, you're helping build our professional community.

And finally, I hope you will consider making a contribution to future editions of True North Resilience. Every day, the Certified Professionals of DRI Canada are leading through creative, innovative, and important work. I hope you will share your lessons and perspectives with your peers who share the goal of a better prepared and more resilient nation.

With sincere thanks for your work.. ■

**N**ous avons beaucoup appris au cours des deux dernières années. Nous savons depuis longtemps que la gestion de la continuité est un élément important de la préparation et de la sécurité de notre pays. La COVID l'a non seulement prouvé, mais elle a également montré aux Canadiens que les professionnels certifiés de DRI Canada fournissent quelque chose d'important qui fait de nos communautés, de nos entreprises et de nos organisations un endroit plus sûr. C'était une urgence unique en une génération, et le travail que nous faisons n'a jamais été aussi important.

De même, le travail de DRI Canada n'a jamais été aussi important. L'avancement de notre profession n'est pas seulement important pour nos professionnels certifiés ... les deux dernières années ont montré que c'est important pour tous les Canadiens. Nous avons vu que notre travail porte vraiment sur la sûreté et la sécurité

publiques, et que ces besoins sont mieux satisfaits grâce à un organisme sans but lucratif solide qui bâtit une communauté de professionnels de la gestion de la continuité.

True North Resilience consiste à bâtir cette communauté. Il s'agit aussi de montrer que notre communauté grandit et évolue.

Notre objectif est d'utiliser ce magazine pour partager des informations qui montrent non seulement le bon travail qui se fait, mais aussi vers l'avenir. Notre travail dans la gestion de la continuité n'a jamais été isolé, et Covid a montré que ces connexions deviennent de plus en plus complexes. Vous verrez que True North Resilience est conçu pour refléter la réalité de notre travail et s'inspire du point de vue des nombreux partenaires qui façonnent le travail que nous faisons et l'orientation de notre profession.

J'aimerais terminer en remerciant les personnes qui ont contribué à faire de True North Resilience une réalité. Plus important encore, j'aimerais souligner le leadership et le travail acharné de Garth Tucker de la part de notre conseil d'administration. Garth a vu le besoin, a construit la vision et a dirigé le travail pour que cela se produise. Merci aussi à tous ceux qui ont contribué à un article. En partageant vos expériences et vos points de vue, vous contribuez à bâtir notre communauté professionnelle.

Enfin, j'espère que vous envisagerez de contribuer aux prochaines éditions de True North Resilience. Chaque jour, les professionnels certifiés de DRI Canada mènent un travail créatif, novateur et important. J'espère que vous partagerez vos leçons et vos points de vue avec vos pairs qui partagent l'objectif d'une nation mieux préparée et plus résiliente.

Avec des remerciements sincères pour votre travail... ■

# Bureau des rédacteurs

## Editors' Desk

By/Par Garth Tucker, CBCP CORP

**T**hank you for being a DRI Canada certified professional! This magazine is dedicated to you and to our chosen profession.

For our profession to grow and become normalized at all levels of business, from small to large, we must work together by sharing knowledge and ensure we provide value to the business. This magazine was designed to include all the various resilience roles found in both public and private sector, from business continuity/disaster recovery to risk, emergency management, security, and OH&S. As we believe that cooperation, shared data, and processes are the future of our profession.

Many businesses see our profession as a cost center, not generating revenue, but that's a very narrow and short-sighted view. Implementing a Resilience Program does absolutely cost the business money, but when you gather the data on business outages, past and projected, then include the savings made possible by mitigation processes introduced by the various practice areas, we more than pay for ourselves. Integrating the various practices data and processes will lead to efficiencies, and most importantly, more resilient organizations.

We had many excellent articles submitted for publication, but we can't include them all in one issue, but they will be used in subsequent issues and on our website as reference materials. If you feel you have something to share which will help improve or promote our profession, please see our submission guidelines, and send your article to [editors@dri.ca](mailto:editors@dri.ca).

Thank you again for supporting us and the profession, we hope you enjoy the knowledge transfer provided by some of the most experienced and skilled professionals in Canada!

True North Resilience Editors ■

**M**erci d'être un professionnel certifié DRI Canada! Ce magazine est dédié à vous et à la profession que nous avons choisie.

Pour que notre profession se développe et se normalise à tous les niveaux de l'entreprise, des plus petits aux plus grands, nous devons travailler ensemble en partageant les connaissances et en nous assurant d'apporter de la valeur à l'entreprise. Ce magazine a été conçu pour inclure tous les différents rôles de résilience que l'on retrouve dans les secteurs public et privé, de la continuité des activités / reprise après sinistre aux risques, à la gestion des urgences, à la sécurité et à la SST. Car nous croyons que la coopération, le partage des données et des processus sont l'avenir de notre profession.

De nombreuses entreprises considèrent notre profession comme un centre de coûts, ne générant pas de revenus, mais c'est une vision très étroite et à courte vue. La mise en œuvre d'un programme de résilience coûte absolument de l'argent à l'entreprise, mais lorsque vous recueillez les données sur les pannes d'entreprise, passées et prévues, puis que vous incluez les économies rendues possibles par les processus d'atténuation introduits par les différents domaines de pratique, nous sommes plus que rentables. L'intégration des diverses données et processus de pratiques mènera à des gains d'efficacité et, surtout, à des organisations plus résilientes.

Nous avons eu beaucoup d'excellents articles soumis pour publication, mais nous ne pouvons pas tous les inclure dans un seul numéro, mais ils seront utilisés dans les numéros suivants et sur notre site Web comme documents de référence. Si vous pensez avoir quelque chose à partager qui vous aidera à améliorer ou à promouvoir notre profession, veuillez consulter nos directives de soumission et envoyer votre article à [editors@dri.ca](mailto:editors@dri.ca).

Merci encore de nous soutenir, nous et la profession, nous espérons que vous apprécierez le transfert de connaissances fourni par certains des professionnels les plus expérimentés et les plus qualifiés au Canada!

Rédacteurs en chef de True North Resilience ■

# Encouraging Credibility and Professionalism

## Encourager la crédibilité et le professionnalisme

**F**or many years, DRI CANADA (DRIC) and DRI International (DRII) have trained and certified professionals in business continuity management (BCM). Our certified professionals have helped hundreds of Canadian organizations to recover effectively from disruptive events. This training and certification has also launched and sustained thousands of successful and rewarding careers. While DRIC training and certification involves an investment of time, effort and money, organizations and individuals stand to profit in both the short- and long-term by capitalizing on its value. Today, hundreds of Canadian organizations insist that their resources rely on DRIC's high caliber training.

By developing a base of common knowledge for the continuity management profession and certifying qualified individuals, DRI encourages credibility and professionalism in the field. ■

**D**epuis de nombreuses années, DRI CANADA (DRIC) et DRI International (DRII) forment et certifient des professionnels en gestion de la continuité des affaires (BCM). Nos professionnels certifiés ont aidé des centaines d'organisations canadiennes à se remettre efficacement d'événements perturbateurs. Cette formation et cette certification ont également permis de lancer et de soutenir des milliers de carrières fructueuses et enrichissantes. Bien que la formation et la certification DRIC impliquent un investissement en temps, en efforts et en argent, les organisations et les individus ont tout à gagner à court et à long terme en capitalisant sur sa valeur. Aujourd'hui, des centaines d'organisations canadiennes insistent pour que leurs ressources s'appuient sur la formation de haut calibre de DRIC.

En développant une base de connaissances communes pour la profession de la gestion de la continuité et en certifiant les personnes qualifiées, DRI encourage la crédibilité et le professionnalisme dans le domaine. ■



EN CAS D'INCIDENT MAJEUR,  
**QUEL EST  
VOTRE PLAN ?**

### NOUS SOMMES LA RÉFÉRENCE

- CONTINUITÉ DES AFFAIRES
- MESURES D'URGENCE
- GESTION DE CRISE
- RELÈVE DE DÉASTRE

*We are located in Quebec but our services are available in English across Canada.*

*Get in touch with us!*



N'attendez pas avant qu'il soit trop tard

**CONTACTEZ-NOUS POUR EN SAVOIR PLUS**

**BR** Benoit Racette  
Services-conseils inc.

Continuité des affaires | Mesures d'urgence  
Gestion de crise | Relève de désastre

 **RACETTECONSEILS.COM**

 **514 312-8474**

 **info@racetteconseils.com**

# Cyberattacks: Stakeholder & Responses, Impacts & Trends (Part 1)

## La montée de la cybercriminalité : Quel est le coût réel? (Première Partie)

By/Par Thibault Dambrine

In this article, I will describe:

- Cyberattack response stakeholder roles and processes

In the next issue, I will describe:

- The impact cyberattacks have on organizations and people
- Risk mitigation investments, points of references and trends

Dans cet article, nous allons enquêter sur :

- Les rôles et processus des intervenants en matière de cyberattaques

Dans le prochain numéro, nous allons couvrir :

- L'impact des cyberattaques sur les organisations et les personnes
- Les investissements possibles pour atténuer les risques, ainsi que des points de référence

**R**isk mitigation investments, points of references and trends At the end of 2019, news of a distant epidemic by the name of "Covid-19" started making headlines. Within a few short weeks, it spread throughout the world. This laptop event triggered a global shift for knowledge workers. To help prevent the virus spread, those who could remain productive using a connected through the Internet were told to work from home.

For most organizations, having workers connect remotely via the Internet on casual basis or for support reasons had always been technically available. Very few organizations, however, were equipped with enough capacity to handle the increased volume required by workers connecting from home due to Covid-19. At that time, many organizations did not use multi-factor authentication (MFA) for external connectivity. Some opened Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC) ports as a temporary measure to accommodate the need for additional remote desktop sessions. This all happened quickly, at the cost of additional cyberattack risk.

In a parallel world, tech-savvy thieves did not fail to notice a massive opportunity. A cybercrime boom was born, complete with a surge in "Ransomware as a Service" (RaaS) attacks, a variation on the "Software as a Service" (SaaS) business model. The 2021 FBI Internet Crime Report shows that between 2019 and 2020 alone, the number of cybersecurity complaints increased by almost 70%.

Today, cybercrimes openly reported in the news are no longer unusual events. What has changed however is that such attacks tend to affect larger number of individuals, stranding airline passengers, causing gasoline shortages,

**V**ers la fin de 2019, une nouvelle épidémie lointaine a commencé à faire les gros titres dans les nouvelles. En quelques semaines, la Covid-19 s'est répandue dans le monde entier. Pour aider à prévenir la propagation du virus, beaucoup ont été encouragés à travailler depuis leur domicile, via l'Internet.

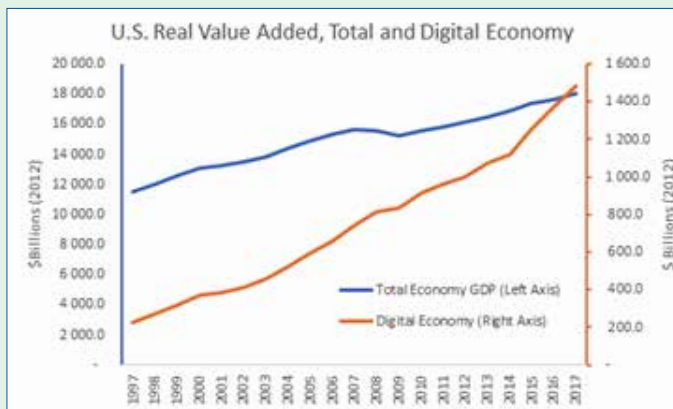
Pour la plupart des organisations, avoir un nombre limité de travailleurs connectés à distance via Internet de manière occasionnelle, ou pour des raisons de soutien, était techniquement établi. Peu d'organisations, cependant, étaient équipées de capacité suffisante pour gérer le volume accru requis pour les travailleurs se connectant depuis leurs domiciles en raison de la Covid-19. De nombreuses organisations n'utilisaient pas l'authentification multi facteur (« multifactor authentication » ou MFA) pour la connectivité externe. Une solution « à court terme » souvent utilisée pour résoudre rapidement ce problème de capacité consistait à ouvrir des ports dits de « bureau à distance » (Remote Desktop Protocol RDP) ou VNC (Virtual Network Computing) comme mesure temporaire, pour répondre au besoin de sessions bureau à distance supplémentaires. En mettant ces mesures en œuvre en urgence, de nombreuses organisations ont augmenté leur risque d'exposition aux cyberattaques.

Les cybercriminels n'ont pas manqué de remarquer une énorme opportunité. Un boom de la cybercriminalité est né, et avec elle, une recrudescence d'attaques à partir de « rançongiciel comme service » ou de « Ransomware as a Service » (RaaS), une variante du modèle économique « Software as a Service » (SaaS). Le FBI Internet Crime Report 2021 montre qu'entre 2019 et 2020 seulement, le nombre de plaintes en matière de cybersécurité a augmenté de près de 70% aux États-Unis. Le reste du monde n'a pas été épargné.

leaking banking customer data, crippling hospitals and more. The damage is real, it is visible, it is far-reaching and it affects people's lives. This is not a "victimless crime".

## Part 1: Cyberattack Stakeholders & Responses

The chart below shows how quickly digital transactions have changed our lives. As a result, the value of the data within has increased significantly. Despite its increased value, data, stored locally, on the Cloud or in movement, remains vulnerable. It must be backed up, protected and constantly monitored for possible corruption. It must be, but is it? Cyberthieves have noticed the vulnerabilities.



Source: <https://www.nist.gov/blogs/taking-measure/cybercrime-its-worse-we-thought>

*Le graphique à gauche reflète la vitesse à laquelle la valeur de l'économie digitale (courbe orange) a augmenté, par rapport à l'économie traditionnelle (courbe bleue)*

The target, in any Cyberattack, is data. At first glance, this appears to be a technical issue, with technical solutions. There are in fact three key additional implications and technical recovery is part of that set. Here is the bigger picture:

### 1) Legal Considerations:

- In Canada, the Personal Information Protection and Electronic Document Act (PIPEDA), mandates reporting breaches where personal information may put individuals at risk.
- As custodian of sensitive client information, a company or organization that is hacked or breached with a cyberattack may be subject to lawsuits from customers, joint-venture partners and other outside stakeholders who were counting on their data to be properly secured.

### 2) Insurance considerations:

- Data, in digital form, has become so integral to most company functions that it is now considered an asset.
  - o Companies, organizations, protect their assets against risk with insurance policies. Buildings and vehicles come to mind. Data, either in motion (think of e-commerce, process control systems) or in storage (think of HR personnel information), is also a working asset which warrants protection.
  - o Insurance companies assess the risk and charge

Aujourd'hui, les cybercrimes ouvertement rapportés dans les nouvelles ne sont plus des événements inhabituels. Ce qui a changé, c'est que de telles attaques ont tendance à affecter un plus grand nombre de personnes, bloquant les passagers de lignes aériennes dans les aéroports, provoquant des pénuries d'essence, divulguant des données sur les dépositaires bancaires, paralysant les hôpitaux et plus encore. Les dégâts sont réels. Ils sont visibles. Ils sont d'une grande portée. Ces crimes affectent la vie des gens. Contrairement à ce que l'on entend trop souvent, ce ne sont pas des « crimes sans victimes ».

## Première Partie : Intervenants et réponses aux cyberattaques

Le graphique à gauche montre à quelle vitesse les transactions numériques ont changé nos vies. En conséquence, la quantité de données que nous partageons personnellement avec les organisations a augmenté et la valeur de ces données a également augmenté de manière significative.

Malgré leur valeur accrue, les données, stockées localement, sur le Cloud ou en mouvements, qui ne sont pas protégées de manière adéquate restent vulnérables aux cybercriminels. Dans cet esprit, les entreprises et les organisations doivent s'assurer qu'elles sont sauvegardées, protégées et constamment surveillées pour détecter d'éventuelles corruptions.

La cible, dans toute cyberattaque, ce sont les données. À première vue, une cyberattaque peut sembler être un problème technique, avec des solutions techniques. Il y a en fait trois implications additionnelles. L'aspect technique n'est qu'une partie de cet ensemble. Voici une vue d'ensemble :

### 1) Considérations relatives aux coûts :

- Implications de l'interruption d'activité - en 2022, le délai moyen entre le chiffrement et la récupération complète du système est d'un mois (voir lien)
- Le coût de la récupération des données et des systèmes - la récupération technique que nous avons décrite précédemment
- Le temps nécessaire pour reconstruire les relations clients existantes
- Le coût supplémentaire de convaincre de nouveaux clients de faire des affaires, après une cyberattaque réussie
- Le coût du paiement de la rançon, si un ransomware et/ou l'extraction de données est impliqué

### 2) Considérations relatives à l'assurance :

- Les données, sous forme numérique, sont devenues si intégrées à la plupart des fonctions de l'entreprise qu'elles sont maintenant considérées comme un « actif », au sens comptable.
  - o Quand on pense à « la protection des actifs »,

premiums for individual types of coverage. Insurance policies aimed at protecting data from the risk of cyberattacks are one of those.

- If a company has a cyber insurance policy at the time when they get hacked, the insurer will no doubt be called and get involved. There is good reason to have data insured. Cyberattack damages can be very expensive.

### 3) Cost Considerations:

- The cost of ransoms, if ransomware or data extraction is involved
- The cost of not being able to do business - in 2021, the average time from encryption to full system recovery is one month. (Source: <https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/> )
- The cost of recovering data and systems – the technical recovery we described earlier on
- The cost of regaining confidence from existing customers
- The additional cost of convincing new customers to do business, after a successful cyberattack

Imagine being an IT manager, coming to work on a Monday morning following a long weekend. The first thing you find out that all the systems you are responsible for are no longer operational. One of the server console screens shows a note describing the terms of a ransom. What's next?

Business is halted. The phone is ringing. There is a sense of urgency to get things fixed quickly. Cyberattack recovery is intricate by nature. Data may be encrypted. It may be compromised. Backup data may be affected as well. Data may have been extracted by the hackers. Applications may no longer be operational. Operating systems may be impacted or modified with back-door access points. HR and personnel data, such as SIN numbers, may be at risk. On minute one, there is no estimated time for recovery. Understanding the extent of the damage takes time. This is a high-stress situation. Data has been leaked, destroyed, altered, or made unusable on your watch.

What type of attacks are we talking about? How do hackers get started? What type of damage do they cause? The following graph provides an overview of entry points and attack methods:

In this scenario, we made the assumption is that the organization has cyber insurance coverage. Once past the initial shock, as the IT manager, you will lead that first phone call to the insurer. The following paragraphs will describe what you may be able to expect past that point. As a start, the insurance company will recommend using two distinct services:

- 1) The immediate technical emergency is a prime concern. A recommendation will be made to hire trusted a third-party

les entreprises, les organisations, protègent leurs actifs contre les risques avec des polices d'assurance. Les bâtiments et les véhicules viennent à l'esprit. Les données sont aussi considérées comme des actifs, qu'elles soient

- En mouvement (pensez au commerce électronique, aux systèmes de contrôle des processus)
- Stockées (pensez aux informations sur le personnel des RH) sont également des actifs fonctionnels qui méritent d'être protégés.

o Pour facturer d'une façon appropriée les primes d'assurance pour différents types d'actif et de couverture, les compagnies d'assurance évaluent les risques. Les polices d'assurance visant à protéger les données contre les risques de cyberattaques font partie de cet ensemble de méthodes.

- En cas d'attaque, si une entreprise détient une police d'assurance pour la cybersécurité, la première étape logique consiste à initier une réclamation sur cet incident contre la police.
  - o Les compagnies d'assurances ont typiquement un nombre de contacts professionnels et experts à leur disposition dans leurs carnets de ressources. Avec cet aide, ils peuvent aider leurs clients à se remettre en ligne plus rapidement, réduire le risque de problèmes juridiques et dans certains cas, gérer les relations de presse autour de l'incident.

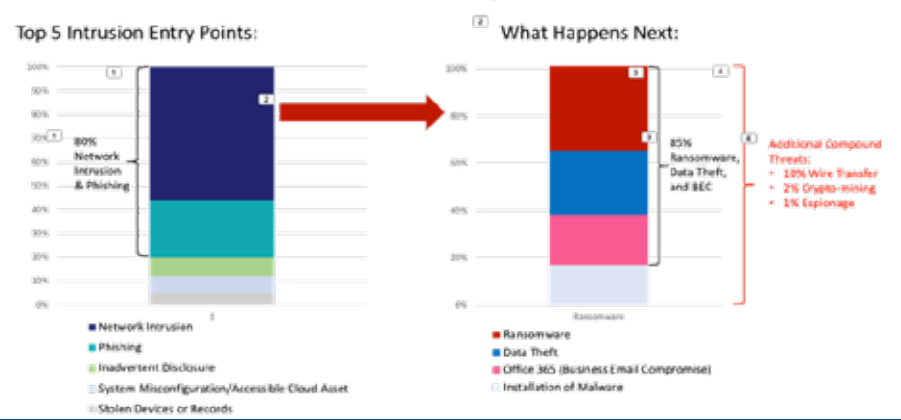
### 3) Considérations juridiques :

- Au Canada, la Loi sur la protection des renseignements personnels et les documents électroniques (Personal Information Protection and Electronic Document Act - PIPEDA) exige le signalement des atteintes à la protection des renseignements personnels lorsque des renseignements personnels peuvent mettre les personnes en danger.
- Un dépositaire d'informations sensibles sur les clients, une entreprise ou une organisation piratée ou violée par une cyberattaque peut faire l'objet de poursuites de la part de clients, de partenaires de coentreprise et d'autres parties prenantes externes qui comptaient sur la sécurité de leurs données.

Imaginez d'être un responsable d'un département d'informatique. Vous venez travailler un lundi matin. La première chose que vous découvrez, c'est que tous les systèmes dont vous êtes responsable ne sont plus opérationnels. L'un des écrans de la console du serveur affiche une note décrivant les conditions d'une rançon. Quelle est la prochaine étape?

Les affaires sont arrêtées. Les téléphones sonnent de partout. Il y a un sentiment d'urgence à régler les choses rapidement. La récupération des cyberattaques est

## 2021 Intrusion and Attack Summary



complexe par nature. Les données peuvent être chiffrées, elles peuvent être compromises et les données de sauvegarde peuvent également être affectées. Des données peuvent avoir été extraites par les pirates. Les applications peuvent ne plus être opérationnelles. Les systèmes d'exploitation peuvent être affectés ou modifiés avec des points d'accès dérobés. Les données sur les RH et le personnel, comme les numéros d'Assurance Sociale ou de compte bancaire, peuvent être à risque.

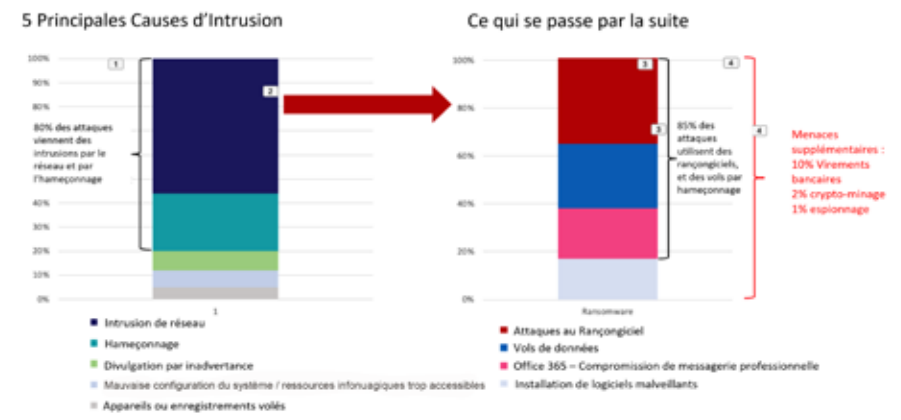
À la première minute, il n'y a pas de temps estimé pour la récupération. Comprendre l'étendue des dégâts prend du temps. Il s'agit d'une situation typiquement très stressante. Des données sensibles peuvent avoir été volées, divulguées, détruites, modifiées ou rendues inutilisables sous votre gouverne.

De quel type d'attaques parle-t-on ? Comment les pirates informatiques commencent-ils ? Quel type de dommages causent-ils ? Le graphique suivant fournit une vue d'ensemble des points d'entrée et des méthodes d'attaque :

Dans ce scénario, nous avons supposé que l'organisation concernée dispose d'une couverture de cyber assurance. Une fois passé le choc initial, en tant que responsable informatique, votre première tâche sera de faire un premier appel téléphonique à votre assureur. Les paragraphes suivants décriront ce à quoi vous pourriez vous attendre au-delà de ce point. Pour commencer, la compagnie d'assurance recommandera d'utiliser deux services distincts :

- 1) L'urgence technique immédiate est une préoccupation majeure. Une recommandation sera faite pour embaucher une société de conseil en cybersécurité tierce de confiance, avec une ou plusieurs des capacités suivantes, en fonction des besoins spécifiques :
  - Experts en récupération de données et de systèmes

## Sommaire des Intrusions et des Cyber Attaques en 2021



cybersecurity consulting company with one or more the following capabilities, depending on the specific requirements:

- Data and system recovery experts
- Ransomware negotiation experience
- Digital forensic experts
- Cybersecurity specialists

Trust, experience and proven competence are key factors in this choice.

2) To coordinate the recovery, which is almost invariably complex, a breach coach will be assigned. The breach coach is almost always a lawyer. This is to address the foreseeable legal issues to come, after a cyberattack, in effect providing both the coaching advice and the legal counsel.

One of the most common risks resulting from a cyberattack is that personal identifiable information (PII)

or personal health information (PHI) may be divulged. In addition, confidential corporate data, such as patents or company secrets may be at risk as well. The role of the breach coach is to guide the organization in identifying the requirements related to data privacy and help advise on retaining a competent, trusted third-party providers to help control and contain post attack damage.

### These include:

- Hiring credit monitoring services
- Advising on public relation strategies and specialists
- Ensuring post breach obligations are satisfied for each of the jurisdictions that the company operates in, as well as the implications.
- In many cases, advise on the decision of what technical recovery service (mentioned in point 1 above) companies may be used.



- Expérience de négociation de ransomware
- Experts en criminalistique numérique
- Spécialistes de la cybersécurité

La confiance, l'expérience et la compétence prouvée sont les facteurs clés dans ce choix.

2) Pour coordonner la récupération, qui est presque toujours complexe, un coach en récupération de cyberattaque (breach coach) sera engagé. Le coach en récupération de cyberattaque est presque toujours un avocat. Il s'agit de résoudre les problèmes juridiques prévisibles à venir, après une cyberattaque, en fournissant en fait à la fois les conseils de guide expérimenté dans ces circonstances et les conseils juridiques.

L'un des risques les plus courants résultant d'une cyberattaque est que des renseignements personnels identifiables (PII) ou des renseignements personnels sur la santé (PHI) puissent être divulgués. En outre, les données confidentielles de l'entreprise, telles que les brevets ou les informations confidentielles de l'entreprise, peuvent également être menacées. Le rôle du coach en récupération de cyberattaque est de guider l'organisation dans l'identification des exigences liées à la confidentialité des données et de l'aider à retenir les fournisseurs compétitifs, de confiance, pour aider à contrôler et à contenir les dommages post-attaque.

#### Il s'agit notamment des éléments suivants :

- Embauche de services de surveillance du crédit
- Conseils sur les stratégies de relations publiques (comment communiquer les circonstances de l'incident)
- S'assurer que les obligations post-violation sont respectées pour chacune des juridictions dans lesquelles la société opère.
- Dans de nombreux cas, conseiller sur le choix de service de récupération technique (mentionné au point 1 ci-dessus).

Le fournisseur de cybersécurité, désigné pour effectuer les services immédiats de récupération de données et de systèmes, effectuera une première évaluation du travail à effectuer et fournira un énoncé des travaux à la compagnie d'assurance. Si cela est approuvé, les travaux de récupération se poursuivront, sous la direction du coach en récupération de cyber-attaque.

Les tâches de récupération post-cyberattaque entrent généralement dans l'une des trois catégories suivantes:

#### 1) Négociations de rançon (si l'utilisation d'un rançongiciel est impliquée)

- Collecte de preuves (entre autres, investiguer si le rançonneur a la réputation de prendre l'argent sans livrer de clef de décryptage ou si le rançonneur est sanctionné par les autorités gouvernementales)

The cybersecurity provider appointed to perform the immediate data and system recovery services will perform a first evaluation on the work to be done and provide a Statement of Work (SoW) to the insurance company. If this is approved, the recovery work will go ahead, under the guidance of the breach coach.

Post-cyberattack recovery tasks typically fall in one of three big categories:

### 1) Ransomware negotiations (if a ransom is involved)

- Evidence collection
- Ransomware negotiation, with the aim of reducing the ransom and still get the decryption key
- Decryption and data recovery

### 2) Forensics (if data has been extracted)

- Evidence collection
- Root-cause investigation, compromise assessment

### 3) Post-breach remediation

- Post-breach evidence collection
- Help and remediation for
  - o Decrypting data
  - o Network vulnerability review
  - o Active Directory /Domain Controller
  - o Hypervisor infrastructure
  - o Email systems vulnerability review
  - o Server re-build
  - o Backup re-build
- Cloud solution security
- e-Discovery
- Dark web search

The scenario above involves an insurance company, a breach coach and an outsourced technical consulting service. Not all companies are insured, nor will they necessarily have access to all these specific resources. Experience shows however that having access to a team of experts, who deal with these issues every day, make recovery significantly less stressful and increase the chances of a speedier recovery. Another element that invariably helps in such circumstances is a well-structured, well-practiced and well-tested disaster recovery plan. ■

**Editors' note: Watch for the second part of this article in the Spring 2023 edition of True North Resilience magazine.**

*Thibault Dambrine is an IT consultant with Keyera Corp. ([keyera.com](http://keyera.com)) in Calgary, Alberta. At the time of writing, he was working for CyberClan ([www.cyberclan.com](http://www.cyberclan.com)). The author thanks each and every reviewer that helped make this essay what it has become. Thibault can be reached at [dambrine@gmail.com](mailto:dambrine@gmail.com).*

- Négociation de rançon, dans le but de réduire le montant de rançon à payer tout en obtenant la clé de décryptage
- Décryptage et récupération de données

### 2) Criminalistique (si les données ont été exfiltrées)

- Collecte de preuves
- Enquête sur les causes profondes, évaluation des compromis

### 3) Correction après la violation

- Collecte de preuves après l'atteinte à la vie privée
- Aide et correction pour
  - o Décryptage des données
  - o Examen de la vulnérabilité du réseau
  - o Active Directory/Contrôleur de domaine
  - o Infrastructure de l'hyperviseur
  - o Examen de la vulnérabilité des systèmes de messagerie
  - o Reconstruction du serveur
  - o Reconstruction de sauvegarde
- Sécurité des solutions Infonuagique
- Découverte électronique (eDiscovery)
- Recherche sur le Dark Web

Le scénario que nous venons de décrire implique une compagnie d'assurance, un coach en récupération de cyber-attaque et un service de conseil technique externe. On ne peut pas prendre toutes ces ressources pour acquis. L'expérience montre cependant que le fait d'avoir accès à une équipe d'experts, qui traitent de ces questions tous les jours, rend le processus de récupération beaucoup moins stressant et augmente les chances d'un rétablissement plus rapide. D'autres éléments qui aident invariablement dans de telles circonstances sont un plan de reprise après sinistre (DRP) bien structuré et bien exercé, un plan de continuité des activités (BCP) et une base de données de gestion de la configuration (CMDB) à jour. ■

**Note de la rédaction : Surveillez la deuxième partie de cet article dans l'édition du printemps 2023 du magazine de Résilience du Vrai Nord.**

*Thibault Dambrine est un consultant en TI chez Keyera Corp. ([keyera.com](http://keyera.com)) à Calgary, en Alberta. Au moment d'écrire cet article, il travaillait chez CyberClan ([www.cyberclan.com](http://www.cyberclan.com)). L'auteur remercie tous les critiques qui ont contribué à faire de cet essai ce qu'il est devenu. Thibault est joignable à [dambrine@gmail.com](mailto:dambrine@gmail.com).*



# Responding to a Disaster Using a Framework

## Intervention en cas de sinistre à l'aide d'un cadre

*By/Par Tim Lalonde*



DR Framework  
Cadré de  
Reprise

**A**s someone who has been in the game too long to admit how long, I can assure you the rules of proper business resilience planning have NOT changed. The demands on the plan have clearly changed but not the need to have and maintain a plan. The traditional method of write-it-once, put-it-on-a-shelf and check it once a year is long gone.

Today, to meet the demands of the issues facing your business, the plan must be fluid and more importantly actionable.

For those who know me, I am a framework and patterns person. I see business challenges as repeatable patterns. To address this, I am a firm believer in building frameworks to address these patterns in an effective manner that can be actioned. See a Problem, Fix a Problem is my mantra.

Business resiliency is more than just a buzzword. Look at the sheer number of organizations today under tremendous stress for they did not have an adequate plan to execute. COVID-19 may be unique as a pandemic, but it is very similar in pattern to being denied access to your buildings from mould, vandalism, structural stress, etc. This is NOT to make light of how serious COVID-19 is. It is real, please wear a mask and adhere to public health guidelines.

For many years I have followed a methodology for business continuity. Over the years I have tuned it and tweaked it to meet the needs of the organizations I was engaged to assist. What I had found was if a framework was deployed and leveraged, responses to incidents become less stressed, more focused, and with a much higher rate of success. The post-mortems become, truly lessons learned and not “witch hunts”.

**U**n Quelqu'un qui est dans le jeu depuis trop longtemps pour admettre depuis combien de temps, je peux vous assurer que les règles d'une bonne planification de la résilience des entreprises n'ont PAS changé. Les exigences du plan ont clairement changé, mais pas la nécessité d'avoir et de maintenir un plan. La méthode traditionnelle consistant à l'écrire une fois, à le mettre sur une étagère et à le vérifier une fois par an a disparu depuis longtemps.

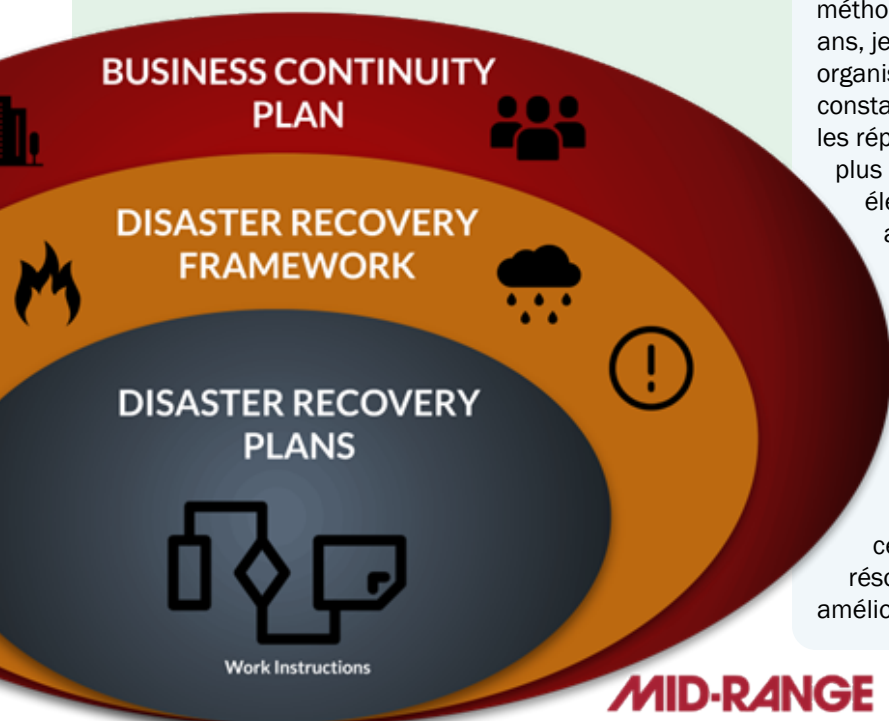
Aujourd'hui, pour répondre aux exigences des enjeux auxquels votre entreprise est confrontée, le plan doit être fluide et surtout réalisable.

Pour ceux qui me connaissent, je suis une personne de cadre et de modèles. Je vois les défis commerciaux comme des modèles reproductibles. Pour y remédier, je crois fermement à l'élaboration de cadres pour aborder ces modèles d'une manière efficace qui peut être mise en œuvre. Voir un problème, résoudre un problème est mon mantra.

La résilience des entreprises est plus qu'un simple mot à la mode. Regardez le nombre d'organisations aujourd'hui soumises à un stress énorme car elles n'avaient pas de plan adéquat à exécuter. La COVID-19 peut être unique en tant que pandémie, mais elle est très similaire à celle qui se voit refuser l'accès à vos bâtiments en raison de moisissures, de vandalisme, de stress structurel, etc. Ce n'est PAS pour faire la lumière sur la gravité de la COVID-19. C'est réel, s'il vous plaît porter un masque et respecter les directives de santé publique.

Pendant de nombreuses années, j'ai suivi une méthodologie pour la continuité des activités. Au fil des ans, je l'ai réglé et modifié pour répondre aux besoins des organisations que j'ai été engagé pour aider. Ce que j'avais constaté, c'est que si un cadre était déployé et exploité, les réponses aux incidents devenaient moins stressantes, plus ciblées et avec un taux de réussite beaucoup plus élevé. Les autopsies deviennent, vraiment des leçons apprises et non des « chasses aux sorcières ».

Pendant toute crise, une gestion de crise appropriée devrait être mise à profit et c'est un sujet pour un autre article. En tant que chefs d'entreprise, nous oublions parfois que pour résoudre un problème, nous devons engager notre personnel. Notre personnel est un être humain qui doit être soigné et protégé en tant que tel en cas de crise. L'atténuation du problème devient le point central, puis une fois qu'il est résolu, une fois qu'il est résolu, une correction appropriée doit être engagée pour améliorer la prochaine réponse à un incident. ➤



During any crisis, proper crisis management should be leveraged and that is a topic for another post. We as business leaders forget at times that to resolve a problem, we need to engage our staff. Our staff are humans that must be cared for and protected as such during a crisis. The mitigation of the issue becomes the focal point, then after it is resolved proper remediation needs to be engaged to improve the next response to an incident.

Now on to the framework. Refer to the graphic as a guide.

### Business Continuity Plan

The Business Continuity Plan is responsible for business interests as a whole entity.

The Business Continuity Plan is the overarching plan to support business interests. It covers elements of staff, buildings, communications, and stakeholders. The components of the BCP include.

- approach
- team compositions
- classification of business services
- physical addresses
- contact trees
- stakeholders
- communication plan

Before you declare a disaster, you refer to the BCP to ensure the executive team is engaged and an appropriate level of approval has been obtained.

It can be as quick as a phone call or it may involve calling in financial and legal teams to confirm the severity of the declaration along with appropriate messaging.

The Business Continuity Plan also refers to business internal and external stakeholders.

### Disaster Recovery Framework

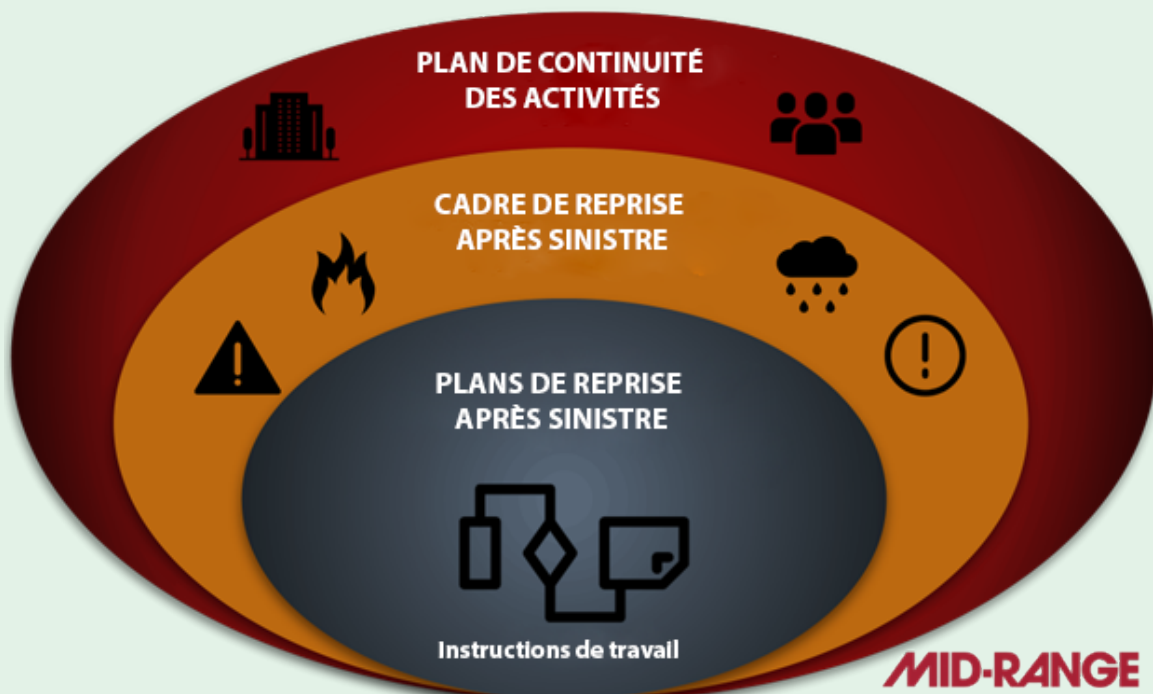
The Disaster Recovery Framework is guided by the Business Continuity Plan and is the actual process to follow.

The Disaster Recovery Framework becomes the execution model for specific Disaster Recover Plans. It is a structured approach to defining the scenarios in both terms of impacted areas, and execution plans but also the definition of completion.

By allowing for a structured approach to recovery, your organization is well-positioned to have a consistent, measurable, and successful recovery from the many different types of technical disaster recovery declarations.

The goal of the Disaster Recovery Framework is to confirm what type of scenario has occurred. A scenario could be one or more of the following.

- Cyberattack
- Pandemic
- Weather/Environmental
- Fire
- No access to business
- Systems failure
- etc.



Passons maintenant au cadre. Reportez-vous au graphique comme guide.

### Plan de continuité des activités

Le plan de continuité des activités est responsable des intérêts commerciaux en tant qu'entité dans son ensemble.

Le plan de continuité des activités est le plan global visant à soutenir les intérêts de l'entreprise. Il couvre les éléments du personnel, des bâtiments, des communications et des parties prenantes. Les composantes du PCA comprennent.

- approche
- compositions d'équipe
- classification des services aux entreprises
- adresses physiques
- arbres de contact
- parties prenantes
- plan de communication

Avant de déclarer une catastrophe, vous vous référez au PCA pour vous assurer que l'équipe de direction est engagée et qu'un niveau approprié d'approbation a été obtenu. Cela peut être aussi rapide qu'un appel téléphonique ou cela peut impliquer d'appeler des équipes financières et juridiques pour confirmer la gravité de la déclaration ainsi que des messages appropriés.

Le plan de continuité des activités fait également référence aux intervenants internes et externes de l'entreprise.

### Cadre de reprise après sinistre

Le cadre de reprise après sinistre est guidé par le plan de continuité des activités et constitue le processus réel à suivre.

L'infrastructure de récupération d'urgence devient le modèle d'exécution pour des plans de récupération d'urgence spécifiques. Il s'agit d'une approche structurée pour définir les scénarios à la fois en termes de zones touchées et de plans d'exécution, mais aussi de définition de l'achèvement.

En permettant une approche structurée de la récupération, votre organisation est bien placée pour disposer d'une récupération cohérente, mesurable et réussie à partir des nombreux types de déclarations techniques de reprise après sinistre.

L'objectif du cadre de récupération d'urgence est de confirmer le type de scénario qui s'est produit. Un scénario peut être l'un ou plusieurs des scénarios suivants.

- Cyberattaque
- Pandémie
- Météo/Environnement
- Incendie
- Pas d'accès aux affaires
- Défaillance des systèmes
- etc.

### Scénarios

Dans le cadre du cadre de reprise après sinistre, les scénarios deviennent l'approche structurée d'un plan de reprise après sinistre spécifique.

Le format de chaque scénario est cohérent pour assurer un meilleur succès lors de l'exécution des plans spécifiques.

Les principaux domaines de chaque scénario sont les suivants:

- Description – Une brève description de l'événement
- Portée – La définition de ce qui est dans et potentiellement hors de portée de l'événement. Cela permet de contenir les plans de rétablissement.
- Zones touchées – Il s'agit d'une liste complète de toutes les applications et/ou composants impliqués dans le scénario. Similaire à la portée mais spécifique aux applications et aux composants.
- Clients touchés – Qui sont les intervenants, les détenteurs de mesures à prendre, les groupes consultés, les groupes informés tant dans les domaines commercial que technique.
- Ressources – Qui sont les ressources internes et externes nécessaires pour compléter le plan.
- Vue d'ensemble de la récupération – Il s'agit de la description de haut niveau des principaux points de contrôle au cours d'un plan de rétablissement.



**MID-RANGE**

Immutable Back Ups  
BUaaS • DRaaS  
High Availability  
Disaster Recovery Tests  
Disaster Recovery Hot Sites  
Disaster Recovery Consulting  
100% Canadian  
Owned & Operated  
Since 1988

midrange.ca  
905-940-1814

SOC 2 TYPE 2  
AICP  
SOC  
MID-RANGE

## Scenarios

As part of the Disaster Recovery Framework, scenarios become the structured approach to a specific Disaster Recovery Plan.

The format of each scenario is consistent to provide for improved success while executing the specific plans.

The major areas of each scenario are;

- Description – A brief description of the event
- Scope – The definition of what is in and potentially out of scope for the event. This allows for containment for the recovery plans.
- Impacted areas – This is a comprehensive list of all applications and/or components involved in the scenario. Similar to scope but specific to applications and components.
- Impacted clients – Who are the stakeholders, action item holders, consulted with groups, informed groups both at the business and technical areas.
- Resources – Who are the resources both internal and external required to complete the plan.
- Recovery Overview – This is the high-level description of the major checkpoints during a recovery plan.
- Major recovery stages (Project Plan) – This is a breakdown of phases with associated tasks to be completed by the plan. It may or may not refer to technical recovery plans.
- Recovery success determination – What is the definition of success as it relates to the recovery.

## Disaster Recovery Plans

The Disaster Recovery Plan is the actual plan to follow wrapped in a specific communications plan.

Typically, this is a formal document, but it can also be a digital tool that lays out the plan to be executed along with a communication plan to keep all stakeholders informed and engaged. I am a firm believer the plan should be digital and in the cloud. That way it is always current and accessible and more importantly, it can be audited.

The contents of a plan may look like the following.

- Control
- Introduction
- Systems and applications
- Execution Plan
  - Milestones
  - Work Instruction(s) to be followed
- Contact List
- Teams
- Results and Findings

## Work Instructions

Work Instructions are very detailed instructions on the actual recovery steps for a specific application and/or component. This is the knowledge base to recovery from a component element all the way up to larger application functions. They may be a small or a very large document that is to be followed.

The instructions should be very complete and NOT rely on internal undocumented knowledge. These Work Instructions are reusable across many Disaster Recovery Plans for they are specific to applications and components. By leveraging a consistent method for these technical instructions, fewer errors are encountered, and a higher level of repeatable success is observed.

The work instructions are potentially used frequently by operations outside of a recovery process. These instructions need to be complete so the individual using the instructions has all they need to complete the task.

## Recovery Flow

The recovery flow is as follows.

- BCP deals with the business
- DRF is the process to follow
- DRPs is the actual execution plan to follow
- Work Instructions are the actual instructions to be followed

## Conclusion

Plan the work and then work the plan. Your plan is the guide to follow. The plan will likely need to change during the execution but not the need to have one. The Disaster Recovery Framework provides a process to follow to ensure all the needs of the business and its stakeholders are accounted for during a recovery event. ■

### **Tim Lalonde**

*Tim Lalonde is the VP of Technical Operations at Mid-Range. He works with leading-edge companies to be more competitive and effective in their industries. He specializes in developing business roadmaps leveraging technology that create and support change from within — with a focus on business process re-engineering, architecture and design, business case development and problem-solving. With over 30 years of experience in IT, Tim's guiding principle remains simple: See a problem, fix a problem.*

- Étapes majeures de rétablissement (plan de projet) – Il s'agit d'une ventilation des phases avec les tâches associées à accomplir par le plan. Il peut ou non faire référence à des plans techniques de rétablissement.
- Détermination du succès du rétablissement – Quelle est la définition du succès en ce qui concerne le rétablissement.

### Plans de reprise après sinistre

Le plan de reprise après sinistre est le plan réel à suivre enveloppé dans un plan de communication spécifique.

En règle générale, il s'agit d'un document formel, mais il peut également s'agir d'un outil numérique qui présente le plan à exécuter ainsi qu'un plan de communication pour tenir toutes les parties prenantes informées et engagées. Je crois fermement que le plan devrait être numérique et dans le cloud. De cette façon, il est toujours à jour et accessible et, plus important encore, il peut être audité.

Le contenu d'un plan peut ressembler à ce qui suit.

- Contrôle
- Introduction
- Systèmes et applications
- Plan d'exécution
  - o Jalons
  - o Instruction(s) de travail à suivre
- Liste de contacts
- Équipes
- Résultats et constatations

### Instructions de travail

Les instructions de travail sont des instructions très détaillées sur les étapes de récupération réelles pour une application et/ou un composant spécifique. Il s'agit de la base de connaissances permettant de récupérer à partir d'un élément de composant jusqu'à des fonctions d'application plus importantes. Il peut s'agir d'un petit ou d'un très grand document à suivre.

Les instructions doivent être très complètes et NE PAS s'appuyer sur des connaissances internes non documentées. Ces instructions de travail sont réutilisables dans de nombreux plans de reprise après sinistre car elles sont spécifiques aux applications et aux composants. En tirant parti d'une méthode cohérente pour ces instructions techniques, moins d'erreurs sont rencontrées et un niveau plus élevé de succès reproductible est observé.

Les instructions de travail sont potentiellement fréquemment utilisées par les opérations en dehors d'un processus de récupération. Ces instructions doivent être complètes afin que la personne qui utilise les instructions ait tout ce dont elle a besoin pour terminer la tâche.

### Flux de récupération

Le flux de récupération est le suivant.

- BCP s'occupe de l'entreprise
- DRF est le processus à suivre
- DRP est le plan d'exécution réel à suivre
- Les instructions de travail sont les instructions réelles à suivre



### Conclusion

Planifiez le travail, puis travaillez le plan. Votre plan est le guide à suivre. Le plan devra probablement changer au cours de l'exécution, mais pas la nécessité d'en avoir un. Le cadre de reprise après sinistre fournit un processus à suivre pour s'assurer que tous les besoins de l'entreprise et de ses parties prenantes sont pris en compte lors d'un événement de récupération. ■

#### **Tim Lalonde**

*Tim Lalonde est vice-président des opérations techniques chez Mid-Range. Il travaille avec des entreprises de pointe pour être plus compétitif et efficace dans leurs industries. Il se spécialise dans l'élaboration de feuilles de route commerciales tirant parti de la technologie qui crée et soutient le changement de l'intérieur, en mettant l'accent sur la réingénierie des processus d'affaires, l'architecture et la conception, le développement d'analyses de rentabilisation et la résolution de problèmes. Avec plus de 30 ans d'expérience en informatique, le principe directeur de Tim reste simple : voir un problème, résoudre un problème.*

# Advancing Table Top Exercise Development: Deliberate Design creates Remarkable Reports

## Faire progresser le développement d'exercices sur table : une conception délibérée crée des rapports remarquables

By/Par Cynthia Wenn, MA CBCP CBCA CRM  
Vanguard Emergency Management Consulting Inc.

### Abstract

According to standards, guidelines and best practices, objectives are the foundation of a dynamic business continuity or emergency management exercise. Many design teams struggle with how to practically apply this idea and fail to grasp the value objectives bring to the report. These problems can be addressed by deploying deliberate design methods. Experience has shown that this begins with investing time to establish objectives of substance and then applying management-by-objectives to exercise design which includes a targeted approach to developing both contextual and contingency injects. This ensures that players are engaged in discussions which concentrate on areas of concern and provide solid information for the report. Then design teams should deliberately implement a variety of standard and creative feedback tools to gather targeted observations. In the after-action report, creators must present quantitative data to dazzle senior management and qualitative information to maximize the value of the exercise to your organization. The article will culminate with five key activities which, if incorporated, will enrich any exercise program.

**Keywords:** after-action report, business continuity management, contextual injects, contingency injects, emergency management, exercise objectives, feedback tools, targeted approach.

### Résumé

Selon les normes, les lignes directrices et les meilleures pratiques, les objectifs constituent le fondement d'un exercice dynamique de continuité des activités ou de gestion des situations d'urgence. De nombreuses équipes de conception ont du mal à savoir comment appliquer concrètement cette idée et ne parviennent pas à saisir la valeur que les objectifs apportent au rapport. Ces problèmes peuvent être résolus en déployant des méthodes de conception délibérées. L'expérience a montré que cela commence par l'investissement de temps pour établir des objectifs de fond, puis l'application de la gestion par objectifs à la conception de l'exercice, ce qui inclut une approche ciblée pour développer des injections contextuelles et d'urgence. Cela garantit que les joueurs sont engagés dans des discussions qui se concentrent sur les domaines de préoccupation et fournissent des informations solides pour le rapport. Ensuite, les équipes de conception devraient délibérément mettre en œuvre une variété d'outils de feedback standard et créatifs pour recueillir des observations ciblées. Dans le rapport après action, les créateurs doivent présenter des données quantitatives pour éblouir la haute direction et des informations qualitatives pour maximiser la valeur de l'exercice pour votre organisation. L'article se terminera par cinq activités clés qui, si elles sont intégrées, enrichiront tout programme d'exercices.

**Mots clés :** rapport après action, gestion de la continuité des activités, injections contextuelles, injections de contingence, gestion des urgences, objectifs de l'exercice, outils de feedback, approche ciblée.

## Deliberate Design

**A** business continuity or emergency management program can stall when an organization invests time and money on exercising but fails to gather meaningful feedback from participants. The term “deliberate design” was first used by **Lisa Maddock** and me to describe a more structured exercise planning method in 2019 at the Continuity and Resilience Today, International Business Continuity Management Conference in Toronto, Canada. Over the past ten years, we have developed and implemented a number of practical tricks for designing participant tools that maximize actionable recommendations and contribute to the creation of an engaging After-Action Review. By engaging in deliberate design, exercise design teams are asked to consider the report at all stages of exercise planning, from initial objective development through tool design and feedback collection.

### Establish Objectives of Substance

*“The exercise objectives are the foundation of the exercise, as they describe the specific outcomes to be achieved and evaluated.”<sup>i</sup>*

Despite being a mandatory feature of exercise design standards and guidelines, design teams often devote little energy to tailoring the objectives to the particular exercise being undertaken. Often, objectives are recycled year over year, for all exercise types, involving any level of the organization. This approach of borrowing or reusing objectives can ensure that the key themes are covered and save time when introducing exercising to an organization. As the program and skill level of the planners mature, it should be apparent that this habit will lead to stale exercises and repetitive reports.

Advanced exercise design teams apply project management principals to each exercise. Developing substantive objectives allows the team to apply a management-by-objectives approach. Management-by-objectives is only effective if everyone involved in the exercise design, facilitation, and play are aware of the objectives. All design team members should be involved in developing the objectives, and all exercise participants (facilitators/controllers, evaluators, observers and players) should be briefed on the objectives prior to exercise play.

There are a number of things to consider when crafting the exercise objectives. Themes are not objectives. Themes are ideas that reoccur in business continuity and emergency management. Objectives identify what should be accomplished in the exercise, but not how or by whom. Concentrate on core competencies involving multiple phases of emergency or continuity management. “Roles and Responsibilities”, “Communication”, or “Plan improvements” are themes within which you may develop objectives, but they are not objectives themselves.

<sup>i</sup> WHO simulation exercise manual. Geneva: World Health Organization; 2017, p.9

## une conception délibérée

**U**n programme de continuité des activités ou de gestion des urgences peut s’enliser lorsqu’une organisation investit du temps et de l’argent dans des exercices, mais ne parvient pas à recueillir des commentaires significatifs auprès des participants. Le terme “conception délibérée” a été utilisé pour la première fois par **Lisa Maddock** et moi pour décrire une méthode de planification d’exercice plus structurée en 2019 lors de la conférence Continuity and Resilience Today, International Business Continuity Management Conference à Toronto, au Canada. Au cours des dix dernières années, nous avons développé et mis en œuvre un certain nombre d’astuces pratiques pour concevoir des outils pour les participants qui maximisent les recommandations exploitables et contribuent à la création d’un bilan après action engageant. En s’engageant dans une conception délibérée, les équipes de conception d’exercices sont invitées à tenir compte du rapport à toutes les étapes de la planification de l’exercice, de l’élaboration des objectifs initiaux à la conception des outils et à la collecte des commentaires.

### Établir les objectifs de la substance

*“Les objectifs de l’exercice constituent le fondement de l’exercice, car ils décrivent les résultats spécifiques à atteindre et à évaluer.”<sup>i</sup>*

Bien qu’il s’agisse d’une caractéristique obligatoire des normes et lignes directrices sur la conception des exercices, les équipes de conception consacrent souvent peu d’énergie à adapter les objectifs à l’exercice particulier qui est entrepris. Souvent, les objectifs sont recyclés d’une année à l’autre, pour tous les types d’exercices, impliquant tous les niveaux de l’organisation. Cette approche consistant à emprunter ou à réutiliser les objectifs permet de s’assurer que les thèmes clés sont couverts et de gagner du temps lors de l’introduction de l’exercice dans une organisation. À mesure que le programme et le niveau de compétence des planificateurs évoluent, il devrait être évident que cette habitude mènera à des exercices périmés et à des rapports répétitifs.

Les équipes de conception d’exercices avancés appliquent les principes de la gestion de projet à chaque exercice. L’élaboration d’objectifs substantiels permet à l’équipe d’appliquer une approche de gestion par objectifs. La gestion par objectifs n’est efficace que si toutes les personnes qui participent à la conception, à l’animation et au déroulement de l’exercice sont au courant des objectifs. Tous les membres de l’équipe de conception devraient participer à l’élaboration des objectifs, et tous les participants à l’exercice (animateurs/contrôleurs, évaluateurs, observateurs et joueurs) devraient être informés des objectifs avant le déroulement de l’exercice.

<sup>i</sup> Manuel d’exercices de simulation de l’OMS. Genève : Organisation mondiale de la santé ; 2017, p.9

Objectives of substance should be SMART (see below) and specifically relate to the team being exercised. Employ verbs that support exercising the people and testing the plans. Objectives need to be numbered and referenced throughout the exercise documentation. They are the foundation for detailed exercise development and are the basis for formal exercise evaluation.

### Smart Objectives

SMART is an acronym used to identify the characteristics of strong objectives. There is disagreement in the industry as to what SMART is an acronym for. The ISO 22398:2013(E) states that objectives should be simple, measurable, achievable, realistic and task-oriented while Homeland Security Exercise Evaluation Program (HSEEP) lists specific, measurable, achievable, relevant and time-bound.

When crafting objectives, consider both lists and note that they agree that objectives must be measurable and achievable.

Il y a un certain nombre d'éléments à prendre en compte lors de l'élaboration des objectifs de l'exercice. Les thèmes ne sont pas des objectifs. Les thèmes sont des idées qui reviennent dans la continuité des opérations et la gestion des urgences. Les objectifs indiquent ce qui doit être accompli dans l'exercice, mais pas comment ni par qui. Concentrez-vous sur les compétences de base impliquant plusieurs phases de la gestion des urgences ou de la continuité. " Rôles et responsabilités ", " Communication " ou " Amélioration des plans " sont des thèmes à l'intérieur desquels vous pouvez élaborer des objectifs, mais ce ne sont pas des objectifs en soi.

Les objectifs de fond doivent être SMART (voir ci-dessous) et se rapporter spécifiquement à l'équipe exercée. Employez des verbes qui appuient l'exercice des personnes et la mise à l'essai des plans. Les objectifs doivent être numérotés et référencés dans toute la documentation de l'exercice. Ils constituent le fondement de l'élaboration détaillée de l'exercice et sont la base de l'évaluation officielle de l'exercice.

### Objectifs intelligents

SMART est un acronyme utilisé pour identifier les caractéristiques des objectifs forts. Il existe un désaccord dans l'industrie quant à la signification de l'acronyme SMART. La norme ISO 22398:2013(E) indique que les objectifs doivent être simples, mesurables, réalisables, réalistes et axés sur les tâches, tandis que le programme d'évaluation des exercices de sécurité intérieure (HSEEP) mentionne des objectifs spécifiques, mesurables, réalisables, pertinents et limités dans le temps.

Lorsque vous élaborer des objectifs, tenez compte des deux listes et notez qu'elles s'accordent sur le fait que les objectifs doivent être mesurables et réalisables. Les objectifs mesurables sont liés à un ensemble de critères permettant d'évaluer le succès. Dans l'exemple fourni, les caractéristiques et les principes du SCI peuvent être utilisés. Lorsque les objectifs ne sont pas

SMART Guidelines for Exercise Objectives Directives SMART pour les objectifs de l'exercice		
<b>Specific</b> Spécifique	Objectives should address the five Ws- who, what, when, where, and why. The objective specifies what needs to be done with a timeline for completion.	Les objectifs doivent répondre aux cinq questions suivantes : qui, quoi, quand, où et pourquoi. L'objectif précise ce qui doit être fait, avec un calendrier d'exécution.
<b>Measurable</b> Mesurable	Objectives should include numeric or descriptive measures that define quantity, quality, cost, etc. Their focus should be on observable actions and outcomes.	Les objectifs doivent inclure des mesures numériques ou descriptives qui définissent la quantité, la qualité, le coût, etc. Ils doivent être axés sur des actions et des résultats observables.
<b>Achievable</b> Réalizable	Objectives should be within the control, influence, and resources of exercise play and participant actions.	Les objectifs doivent se situer dans les limites du contrôle, de l'influence et des ressources du jeu d'exercice et des actions des participants.
<b>Relevant</b> Pertinent	Objectives should be instrumental to the mission of the organization and link to its goals or strategic intent.	Les objectifs doivent contribuer à la mission de l'organisation et être liés à ses buts ou à son intention stratégique.
<b>Time-bound</b> Limité dans le temps	A specified and reasonable timeframe should be incorporated into all objectives.	Un calendrier précis et raisonnable doit être intégré à tous les objectifs.

Table 1 Reference Table 3.1 Homeland Security Exercise Evaluation Program (HSEEP)

Tableau 1 Tableau de référence 3.1 Programme d'évaluation des exercices de sécurité intérieure (HSEEP)

Measurable objectives link to a set of criteria against which success is assessed. In the example provided, the ICS Features and Principles can be used. When the objectives are not measurable, the report cannot truly indicate whether the objectives have been met. Unachievable objectives will frustrate both the design team and the players, sabotaging the exercise.

### Align Players and Objectives

The particular players in the exercise should be factored into the objective development. Objectives must be broad enough to ensure that all players are able to contribute to success. The objectives must be geared to the organizational level of the exercise players. An executive exercise should have strategic objectives. Exercises targeted to operational teams and tactical teams should have more functional and activity focused objectives. If the exercise involves multiple levels, the objectives should be targeted to the most senior level.

**REMEMBER:** the most senior player in the exercise should sign-off on the objectives prior to further exercise development.

### Language

Use verbs that reinforce exercising the people and testing the plans. By choosing verbs that imply judgement, players may perceive that their performance is being evaluated. This will stifle creative problem solving and limit participation.

#### To Use

- Determine
- Develop
- Finalize
- Identify
- Provide
- Prioritize
- Validate
- Verify

#### Not to Use

- Appraise
- Assess
- Evaluate
- Continue
- Critique
- Judge
- Monitor
- Rate

### Example of a SMART objective for a business continuity exercise

Objective #1: Identify opportunities to enhance the use of the Incident Command System by the Incident Management Team to recover time critical services during a disruption lasting more than five days.

**NOTE: All other examples in this article target on this objective.**

mesurables, le rapport ne peut pas vraiment indiquer si les objectifs ont été atteints. Des objectifs inatteignables frustreront à la fois l'équipe de conception et les joueurs, sabotant ainsi l'exercice.

### Aligner les acteurs et les objectifs

Les acteurs particuliers de l'exercice doivent être pris en compte dans l'élaboration des objectifs. Les objectifs doivent être suffisamment larges pour que tous les joueurs puissent contribuer au succès. Les objectifs doivent être adaptés au niveau organisationnel des joueurs de l'exercice. Un exercice destiné aux cadres devrait avoir des objectifs stratégiques. Les exercices destinés aux équipes opérationnelles et aux équipes tactiques devraient avoir des objectifs plus fonctionnels et axés sur les activités. Si l'exercice fait intervenir plusieurs niveaux, les objectifs devraient être axés sur le niveau le plus élevé.

**N'OUBLIEZ PAS :** l'acteur le plus haut placé dans l'exercice devrait approuver les objectifs avant de poursuivre le développement de l'exercice.

### Langue

Utilisez des verbes qui renforcent le fait d'exercer les personnes et de tester les plans. En choisissant des verbes qui impliquent un jugement, les joueurs peuvent avoir l'impression que leurs performances sont évaluées. Cela étouffe la résolution créative des problèmes et limite la participation.

#### A utiliser

- Déterminer
- Développer
- Finalisez
- Identifier
- Fournir
- Donner la priorité à
- Valider
- Vérifier

#### A ne pas utiliser

- Évaluer
- Évaluer
- Évaluer
- Continuer
- Critique
- Juge
- Moniteur
- Taux

### Exemple d'un objectif SMART pour un exercice de continuité des activités

Objectif n° 1 : Identifier les possibilités d'améliorer l'utilisation du système de commandement des incidents par l'équipe de gestion de l'incident pour rétablir les services essentiels pendant une perturbation de plus de cinq jours .

**NOTE : Tous les autres exemples de cet article visent cet objectif.**

## Develop Injects Deliberately

The time allotted for exercise play is limited, so make each inject count. Unfortunately, many exercise design teams fail to create targeted injects. Instead, they follow a “narrative” or “gotcha” approach to inject development.

### Narrative Approach

When design teams use a narrative approach to developing injects, the injects are often based upon how well they add context to the story being presented. While brainstorming, team members will choose to include contextual injects that moves the narrative forward without considering if this information helps the players achieve an aspect of the objective(s). Injects that do not relate to the main plot are not considered. This can lead to the inclusion of many injects that are for information only. Valuable exercise time is wasted as players focus on internalizing this non relevant information.

### Gotcha Approach

When design teams use a gotcha approach to developing injects, the injects add unnecessary layers of difficulty that may make it impossible for the exercise objectives to be met. The design team tries to push the players beyond what they are capable of. This does not support players to practice implementing plans, processes and procedures in a non-threatening environment. Instead, the inclusion of unrealistic or overwhelming injects may be seen as an attempt to demonstrate how the players will fail. Exercise discussions will become scattered and choppy. Players may become frustrated and discouraged. Post exercise, they may feel unprepared and be less likely to want to participate in future exercises.

### Targeted Approach

When design teams use a targeted approach to developing injects, players are engaged in discussions which concentrate on the outcome and distill information for the report. Targeted injects may be contextual, but only if they support resolution of the objectives.

If the players have lost focus on the objectives it may be necessary for the facilitator/controller to introduce contingency injects. In our example below, if the players have not considered resource management, which is a key feature of the incident command system, then the facilitator is prompted to deliver the contingency inject. Targeted contingency injects can also provide players with additional opportunities to achieve objectives if their initial discussions have not been robust. Where the information provided in an inject is loosely tied to an objective, the connection can be embedded within facilitator prompts.

Targeted injects ensure all players are engaged and feel that the exercise is a valuable use of their time. The design team should determine whether they have provided an adequate number of targeted injects to allow for the successful resolution of the objectives. The inject development form must capture the inject recipient and identify the objective(s) it is intended to address. When predicting the outcome of each inject, consider which players will contribute to resolutions. Every player should be prompted to contribute to the resolution of one, some, or even all of the objectives.

### Deploy Feedback Tools Deliberately

It is the responsibility of the design team to ensure that all exercise participants can provide valuable feedback for the report. Employ multiple tools during each exercise to

ensure that feedback is obtained from people with different personality types. Introverts and extroverts respond favorably to different feedback-gathering techniques. Advanced design teams obtain individual and group responses and employ more creative instruments. Leverage tools that provide evaluators with both instant or delayed feedback

#### Example of a Targeted CONTINGENCY Inject

IF the Incident Management Team has not thoroughly considered resource management, THEN provide this inject.

**Objective: 1**

**Recipient:** IMT - Operations

**Inject Description:** The business owner of a time critical service has called with news that 14 laptops appear to have been stolen from their alternate site.

#### Example of a Targeted CONTEXTUAL Inject

**Objective: 1**

**Recipient:** Incident Commander (IC)

**Inject Description:** You have come down with a severe case of the seasonal flu and cannot act as Incident Commander on Day 2.

**Facilitator prompt:** Contact your back-up and initiate a transfer of command.

The initial IC must transfer command (one of the features and principles of ICS).

**CONTINGENCY INJECTS** are events that a controller provides to a player if the players get off track or do not take an action that is necessary for the continuation of the exercise. This ensures that play moves forward, as needed, to adequately evaluate performance of activities. **HSEEP Glossary-2**

## Développer Injecte Délibérément

Le temps alloué à l'exercice est limité, alors faites en sorte que chaque injection compte. Malheureusement, de nombreuses équipes de conception d'exercices ne parviennent pas à créer des injections ciblées. Au lieu de cela, elles adoptent une approche " narrative " ou " attrape-nigaud " pour l'élaboration des injections.

### Approche narrative

Lorsque les équipes de conception utilisent une approche narrative pour développer les injections, les injections sont souvent basées sur la façon dont elles ajoutent un contexte à l'histoire présentée. Lors du brainstorming, les membres de l'équipe choisiront d'inclure des injections contextuelles qui font avancer le récit sans se demander si ces informations aident les joueurs à atteindre un aspect de l'objectif ou des objectifs. Les injections qui ne sont pas liées à l'intrigue principale ne sont pas prises en compte. Cela peut conduire à l'inclusion de nombreux injections qui ne sont que des informations. Un temps d'exercice précieux est perdu lorsque les joueurs se concentrent sur l'internalisation de ces informations non pertinentes.

### L'approche Gotcha

Lorsque les équipes de conception utilisent une approche "gotcha" pour développer des injections, celles-ci ajoutent des couches de difficulté inutiles qui peuvent rendre impossible l'atteinte des objectifs de l'exercice. L'équipe de conception essaie de pousser les joueurs au-delà de ce dont ils sont capables. Cela n'aide pas les joueurs à s'exercer à mettre en oeuvre des plans, des processus et des procédures dans

un environnement non menaçant. Au contraire, l'inclusion d'injections irréalistes ou écrasantes peut être perçue comme une tentative de démontrer comment les joueurs vont échouer. Les discussions de l'exercice deviendront dispersées et hachées. Les joueurs peuvent être frustrés et découragés. Après l'exercice, ils peuvent se sentir mal préparés et être moins enclins à vouloir participer à de futurs exercices.

### Approche ciblée

Lorsque les équipes de conception utilisent une approche ciblée pour développer les injections, les joueurs sont engagés dans des discussions qui se concentrent sur le résultat et distillent des informations pour le rapport. Les injections ciblées peuvent être contextuelles, mais seulement si elles soutiennent la résolution des objectifs.

Si les joueurs ne se concentrent plus sur les objectifs, l'animateur/ contrôleur peut être amené à introduire des injections d'urgence. Dans l'exemple ci-dessous, si les joueurs n'ont pas envisagé la gestion des ressources, qui est un élément clé du système de commandement des interventions, l'animateur est invité à procéder à une injection de contingence. Les injections d'urgence ciblées peuvent également fournir aux joueurs des occasions supplémentaires d'atteindre les objectifs si leurs discussions initiales n'ont pas été solides. Lorsque les informations fournies dans une injection sont vaguement liées à un objectif, le lien peut être intégré dans les invites du facilitateur.

Les injections ciblées permettent de s'assurer que tous les joueurs sont engagés et ont le sentiment que l'exercice est une utilisation valable de leur temps. L'équipe

de conception doit déterminer si elle a prévu un nombre suffisant d'injections ciblées pour permettre la résolution des objectifs. Le formulaire de développement de l'injection doit saisir le destinataire de l'injection et identifier le ou les objectifs qu'elle vise à atteindre. Lorsque vous prévoyez le résultat de chaque injection, tenez compte des joueurs qui contribueront aux résolutions. Chaque joueur doit être invité à contribuer à la résolution d'un, de plusieurs, voire de tous les objectifs.

### Exemple d'une injection ciblée de CONTINGENCY

**SI l'équipe de gestion de l'incident n'a pas envisagé de manière approfondie la gestion des ressources, ALORS fournissez cette injection.**

**Objectif : 1**

**Bénéficiaire : ESI - Opérations**

**Description de l'injection : Le propriétaire d'un service à temps critique a appelé pour annoncer que 14 ordinateurs portables semblent avoir été volés sur leur autre site.**

### Exemple d'une injection CONTEXTUELLE ciblée

**Objectif: 1**

**Bénéficiaire :** Commandant de l'incident (CI)

**Injecter la description :** Vous avez contracté une grippe saisonnière sévère et ne pouvez pas agir en tant que commandant de l'incident au jour 2.

Invitation à l'animateur : Contactez votre remplaçant et initiez un transfert de commandement.

Le CI initial doit transférer la commande (l'une des caractéristiques et des principes de l'ICS).

**Les INJECTS DE CONTINUITÉ sont des événements qu'un contrôleur fournit à un joueur si celui-ci s'égaré ou ne prend pas une mesure nécessaire à la poursuite de l'exercice. Cela permet de s'assurer que le jeu avance, au besoin, pour évaluer adéquatement la performance des activités. *HSEEP Glossaire-2***

on objectives. If you suspect that some topics might be sensitive or have internal political implications, build a mechanism to allow for anonymity. Regardless of the tools deployed, exercise project teams need to track and report on participation and follow-up when needed.

### Instant Feedback Tools

Instant feedback involves getting live or real-time answers during the exercise. Both high and low technology methods of live polling can be used. The simplest is the vote or show of hands. High tech solutions can involve clicker-based polling systems or cellphone applications. They can be free or paid. For more dynamic teams, feedback questions can be posted at the top of whiteboards or flipcharts around the room. Players are encouraged to post feedback on the wall during exercise play. For this method to be successful, the facilitation team must remind the players of this tool when appropriate.

When feedback is provided while the exercise is underway, all participants can ensure that objectives are being met. The facilitator is able leverage the contingency injects if the flipchart associated with one of the objectives is empty or if players are hesitant during a show of hands. If only delayed feedback methods are employed, facilitators may not be able to recognize when players have failed to achieve one or more of the objectives until long after the exercise has ended.

Instant feedback is a quick and easy way for the participants to provide data. Compiling the information should be simple. Limit survey questions to either/or responses. The design team must ensure that tracking and monitoring of instant feedback is captured on an ongoing or continuous basis. By deploying a tech-based polling method, the results are instantly tallied and stored. Provision of instant reaction is often visible to the entire team, allowing for quick validation from the group.

Unfortunately, excessive surveys can disrupt exercise flow and detract from realism. Live results could be skewed positively or negatively by crowd-think or other social behavior. High tech solutions are subject to malfunction and privacy risks.

All exercises should include a verbal debrief at the end of action, encouraging feedback from all participants. The most senior individual in the room should be the last to provide input, as their opinion may taint the response of others. Make certain that scribes capture all information provided in the debrief and/or record it. It will be valuable for the report, although this initial 'gut reaction' can be more difficult for report writers to sort by objective. Verbal feedback can be provided by individuals or by preidentified teams. Teams will require additional time to discuss and then share with the room.

Some feedback gathering methods are undertaken during the exercise but not collected until after play has ended. These include:

- Feedback forms distributed and gathered during the exercise or before players leave the room,
- Concealed surveys,
- Scribe notes,
- Observer feedback packages, and
- Instances of 'encouraged vandalism.'

Encouraged vandalism is when players are asked to scribble on, scratch out and otherwise make changes to plans or reference documents provided to the teams at the exercise. In addition to providing relevant and actionable recommendations, this reminds planners and players that plans and tools are living documents, not sacred text. 'Vandalized' documentation is gathered after the exercise and used to support the appropriate objective(s).

**Exercise in a Box**

**An economical way to deliver a tabletop exercise.**

This kit contains over 40 comprehensive tools. Leverage our plans, templates, and checklists to coach your team with confidence.

**INCLUDES:**

- Scope and Objectives
- Participant Guidelines
- Scenario
- Injects
- Evaluator Package
- Report Templates
- And much more...

**\$1499**

**Vanguard**  
emergency.com

training@vanguardemergency.com  
Mitigation • Response • Continuity • Recovery

### Survey Question Example

Did the information provided during the transfer of command provide all key information required to recover time critical services?

## Déployer délibérément des outils de rétroaction

Il incombe à l'équipe de conception de veiller à ce que tous les participants à l'exercice puissent fournir des commentaires utiles pour le rapport. Utilisez plusieurs outils au cours de chaque exercice pour vous assurer que le feedback est obtenu de personnes ayant des types de personnalité différents. Les introvertis et les extravertis répondent favorablement à différentes techniques de collecte de commentaires. Les équipes de conception avancées obtiennent des réponses individuelles et collectives et utilisent des instruments plus créatifs. Exploitez les outils qui fournissent aux évaluateurs un retour d'information instantané ou différé sur les objectifs. Si vous pensez que certains sujets peuvent être sensibles ou avoir des implications politiques internes, mettez en place un mécanisme permettant l'anonymat. Quels que soient les outils déployés, les équipes de projet de l'exercice doivent suivre la participation, en rendre compte et assurer un suivi si nécessaire.

## Outils de feedback instantané

Le feedback instantané consiste à obtenir des réponses en direct ou en temps réel pendant l'exercice. On peut utiliser des méthodes de sondage en direct de haute et de basse technologie. La plus simple est le vote ou le vote à main levée. applications pour téléphones portables. Elles peuvent être gratuites ou payantes. Pour les équipes plus dynamiques, des questions de rétroaction peuvent être affichées en haut des tableaux blancs ou des tableaux à feuilles mobiles dans la salle. Les joueurs sont encouragés à poster des commentaires sur le mur pendant l'exercice. Pour que cette méthode soit efficace, l'équipe d'animation doit rappeler cet outil aux joueurs au moment opportun.

Lorsque le feedback est fourni pendant le déroulement de l'exercice, tous les participants peuvent s'assurer que les objectifs sont atteints. L'animateur est en mesure de tirer parti des injections d'urgence si le tableau de papier associé à l'un des objectifs est vide ou si les joueurs hésitent lors d'un vote à main levée. Si seules des méthodes de rétroaction différée sont employées, les animateurs peuvent ne pas être en mesure de reconnaître que les joueurs n'ont pas atteint un ou plusieurs des objectifs avant que l'exercice ne soit terminé.

Le feedback instantané est un moyen rapide et facile pour les participants de fournir des données. La compilation des informations doit être simple. Limitez les questions de l'enquête à des réponses de type soit/soit. L'équipe de conception doit veiller à ce que le suivi et la surveillance du feedback instantané soient assurés de manière continue ou permanente. En déployant une méthode de sondage basée sur la technologie, les résultats sont instantanément comptabilisés et stockés. Les réactions instantanées sont souvent visibles par l'ensemble de l'équipe, ce qui permet une validation rapide de la part du groupe.

Malheureusement, des sondages excessifs peuvent perturber le déroulement de l'exercice et nuire au réalisme. Les résultats en direct peuvent être faussés positivement ou négativement par la pensée de la foule ou d'autres comportements sociaux. Les solutions de haute technologie sont sujettes à des dysfonctionnements et à des risques pour la vie privée.

Tous les exercices doivent inclure un débriefing verbal à la fin de l'action, encourageant le retour d'information de tous les participants. La personne la plus expérimentée dans la salle doit être la dernière à apporter sa contribution, car son opinion peut fausser la réponse des autres. Veillez à ce que les scribes saisissent toutes les informations fournies lors du débriefing et/ou les enregistrent. Elles seront précieuses pour le rapport, bien que cette "réaction instinctive" initiale puisse être plus difficile à trier par objectif pour les rédacteurs du rapport. Le feedback verbal peut être fourni par des individus ou par des équipes pré-identifiées. Les équipes auront besoin de plus de temps pour discuter et ensuite partager avec la salle.

Certaines méthodes de collecte de commentaires sont utilisées pendant l'exercice mais ne sont recueillies qu'après la fin du jeu. Il s'agit notamment des méthodes suivantes

- Des formulaires de retour d'information sont distribués et recueillis pendant l'exercice ou avant que les joueurs ne quittent la salle,
- Enquêtes cachées,
- Notes du scribe,
- les dossiers de retour d'information des observateurs, et
- Des cas de "vandalisme encouragé".

On parle de vandalisme encouragé lorsque les joueurs sont invités à gribouiller, gratter et apporter d'autres modifications aux plans ou aux documents de référence fournis aux équipes lors de l'exercice. En plus de fournir des recommandations pertinentes et exploitables, cela rappelle aux planificateurs et aux joueurs que les plans et les outils sont des documents vivants, et non des textes sacrés. La documentation "vandalisée" est recueillie après l'exercice et utilisée pour appuyer le ou les objectifs appropriés.

### Exemple de question d'enquête

**Les informations fournies lors du transfert de commandement ont-elles permis d'obtenir toutes les informations clés nécessaires au rétablissement des services**



### Delayed Feedback Tools

Delayed feedback refers to information gathered post exercise. Impressions can be gathered using feedback forms, surveys, email follow-up, interviews or next-day facilitated workshops. As with instant feedback, there are merits and challenges to consider.

*“Holding in-depth interviews is the best way to really find out what participants thought of the exercise, their own and others’ actions and what they might have learned. In-depth interviews are conducted in order to find out participants’ feelings, thoughts and intentions, which are obviously difficult to observe.” ii*

Exercise participants may be more mentally fit to provide feedback if they are not drained by the exercise conditions themselves. Employing delayed feedback methods could reduce the amount of meeting time assigned to the exercise. If room space or participant time is limited, more time can be devoted to exercise play.

When providing delayed feedback, participants have the opportunity to consider more in depth or complex questions. Only through delayed feedback can you expect that participants respond with detailed documentation enhancements, page numbers or reference to specific figures. Only in delayed feedback questions can you reference page numbers or specific figures, or ask participants to reach out to individuals that were not involved in the exercise.

### Outils de rétroaction différée

Le feedback différé fait référence aux informations recueillies après l'exercice. Les impressions peuvent être recueillies à l'aide de formulaires de retour d'information, d'enquêtes, de suivi par e-mail, d'entretiens ou d'ateliers animés le lendemain. Comme pour le feedback instantané, il y a des avantages et des défis à prendre en compte.

*“La réalisation d’entretiens approfondis est le meilleur moyen de savoir ce que les participants ont pensé de l’exercice, de leurs propres actions et de celles des autres, et ce qu’ils ont pu apprendre. Les entretiens approfondis sont réalisés afin de connaître les sentiments, les pensées et les intentions des participants, qui sont évidemment difficiles à observer.” ii*

Les participants à l'exercice peuvent être plus aptes mentalement à fournir un feedback s'ils ne sont pas épuisés par les conditions de l'exercice elles-mêmes. L'utilisation de méthodes de feedback différé pourrait réduire le temps de réunion consacré à l'exercice. Si l'espace de la salle ou le temps des participants est limité, on peut consacrer plus de temps à l'exercice.

En fournissant un feedback différé, les participants ont la possibilité de réfléchir à des questions plus approfondies ou plus complexes. Ce n'est que par le biais du feedback différé que vous pouvez attendre des participants qu'ils répondent par des améliorations détaillées de la documentation, des numéros de page ou des références

ii Handbook on evaluation of exercises. Karlstad: Swedish Civil Contingencies Agency (MSB); 2011 p.47

ii Manuel sur l'évaluation des exercices. Karlstad : Agence suédoise pour les contingences civiles (MSB) ; 2011 p.47

Unfortunately, there is a high risk that participants will not submit responses, as they have moved on to other tasks. Incentives can help increase response rates. For example, offer to enter all participants who submit a feedback form into a draw for an inexpensive emergency management tool (such as a flashlight, or be prepared kit). If response rates are too low, the value of the report can be compromised. Collecting delayed feedback can be labor intensive, as the report writer may need to undertake significant follow up. The additional time required to overcome these challenges can impede report dissemination and implementation of the recommendations.

### Deliberately Designed Feedback Forms

Feedback forms are the hammer in the toolbox that no design team should be without. Unfortunately, they often do not put very much thought into their content or format. This leads to the inclusion of, at best, pointless questions and, at worst, self-serving ones.

*“Evaluation forms are a good method of harvesting a large quantity of impressions, reflections from participants from the exercise...” iii*

If the questions centre entirely on rating the exercise like a movie review, designers will forfeit gathering substantive data to meet the objectives.

### Content

Questions put forward on the forms or surveys should reflect the approved objectives. In some cases, it can just be a matter of rephrasing the objective into the form of a question. In other cases, it may be necessary to break the

à des figures spécifiques. Ce n'est que dans les questions de feedback différé que vous pouvez faire référence à des numéros de page ou à des figures spécifiques, ou demander aux participants de s'adresser à des personnes qui n'ont pas participé à l'exercice.

Malheureusement, le risque est grand que les participants ne soumettent pas de réponses, car ils sont passés à d'autres tâches. Les incitations peuvent aider à augmenter les taux de réponse. Par exemple, proposez à tous les participants qui soumettent un formulaire de retour d'information de participer au tirage au sort d'un outil de gestion des urgences peu coûteux (comme une lampe de poche ou un kit de préparation). Si les taux de réponse sont trop faibles, la valeur du rapport peut être compromise. La collecte de commentaires tardifs peut demander beaucoup de travail, car le rédacteur du rapport peut avoir à effectuer un suivi important. Le temps supplémentaire nécessaire pour surmonter ces difficultés peut entraver la diffusion du rapport et la mise en oeuvre des recommandations.

### Formulaires de retour d'information délibérément conçus

Les formulaires de retour d'information sont le marteau de la boîte à outils dont aucune équipe de conception ne devrait se passer. Malheureusement, leur contenu et leur format sont souvent peu réfléchis. Cela conduit à l'inclusion, au mieux, de questions inutiles et, au pire, de questions intéressées.

*“Les formulaires d'évaluation sont une bonne méthode pour récolter une grande quantité d'impressions, de réflexions des participants à l'exercice...” iii*

### Examples of QUANTITATIVE AND QUALITATIVE QUESTIONS

**Objective #1:** Identify opportunities to enhance the use of the Incident Command System by the Incident Management Team to recover time critical services during a disruption lasting more than five days.

#### Quantitative Question:

Was the Incident Management Team able to leverage the Incident Command System to recover critical services during the exercise? Yes/Somewhat/No

#### Qualitative Question:

As a member of the Incident Management Team, outline how the Incident Command System can be leveraged to more effectively recover critical services during a disruption lasting more than five days.

### Exemples de QUESTIONS QUANTITATIVES ET QUALITATIVES

**Objectif n° 1 :** identifier les possibilités d'améliorer l'utilisation du système de commandement des incidents par l'équipe de gestion des incidents pour rétablir les services essentiels pendant une perturbation de plus de cinq jours.

#### Question quantitative :

L'équipe de gestion des incidents a-t-elle pu tirer parti du système de commandement des incidents pour rétablir les services essentiels pendant l'exercice ? Oui/Un peu/Non

#### Question qualitative :

En tant que membre de l'équipe de gestion de l'incident, décrivez comment le système de commandement de l'incident peut être utilisé pour rétablir plus efficacement les services essentiels pendant une interruption de plus de cinq jours.

objective down into its parts. Include at least two questions per objective, one qualitative and one quantitative.

Quantitative questions provide report writers with numeric data that can be presented as chart or figures. They ask players to rate on a scale or answer yes/no/maybe. Executives respond well to the visual presentation of quantitative responses in the report.

Qualitative questions are open ended and encourage respondents to elaborate on the issues. The bulk of the data that will be used to create observations in the report comes from responses to these questions. Words to use in the qualitative questions: how can, what can, describe, explain, list, or comment on.

### Format

Printed copies of feedback forms should include adequate spaces for participants to capture their thoughts. All qualitative questions should be followed by a box at least six lines in height. Arrange the questions in order of importance. If questions appear on a second page, the facilitator must bring this to the attention of participants. Many will not turn the page over. Consider using a bright, distinct paper colour for feedback forms, such as yellow or orange. This prevents sheets from getting lost or 'walking' out of the room.

## Create a Remarkable Report

By deliberately designing the exercise to accomplish the objectives, the team should have a straightforward task writing a remarkable after-action report. The executive summary should indicate clearly if the exercise has accomplished each of the objectives. It should present the strongest evidence that the resources were well spent on the exercise.

Si les questions sont entièrement centrées sur l'évaluation de l'exercice comme une critique de film, les concepteurs ne recueilleront pas de données substantielles pour atteindre les objectifs.

### Contenu

Les questions posées sur les formulaires ou les enquêtes doivent refléter les objectifs approuvés. Dans certains cas, il suffit de reformuler l'objectif sous la forme d'une question. Dans d'autres cas, il peut être nécessaire de décomposer l'objectif en ses parties. Incluez au moins deux questions par objectif, une qualitative et une quantitative.

Les questions quantitatives fournissent aux rédacteurs de rapports des données numériques qui peuvent être présentées sous forme de tableau ou de chiffres. Elles demandent aux lecteurs de se situer sur une échelle ou de répondre par oui/non/peut-être. Les cadres réagissent bien à la présentation visuelle des réponses quantitatives dans le rapport.

Les questions qualitatives sont ouvertes et encouragent les répondants à élaborer sur les problèmes. La majeure partie des données qui seront utilisées pour créer des observations dans le rapport provient des réponses à ces questions.

Mots à utiliser dans les questions qualitatives : comment peut-on, que peut-on, décrire, expliquer, énumérer ou commenter.

### Format

Les copies imprimées des formulaires de retour d'information doivent comporter des espaces suffisants pour permettre aux participants de noter leurs réflexions. Toutes les questions qualitatives doivent être suivies d'un encadré d'au moins six lignes de hauteur. Classez les questions par ordre d'importance. Si les questions apparaissent sur une deuxième page, l'animateur doit

## OBSERVATION, LESSON IDENTIFIED AND RECOMMENDATION EXAMPLES

Observation	Lesson Identified	Recommendation
Participants found that alternates were not receiving a comprehensive briefing during the hand over of command	When command is transferred, the process must include a briefing that captures all essential information for continuing safe and effective operations or data will be lost.	Review and formalize the transfer of command process. Outline responsibilities of the outgoing and incoming Incident Commander and situation briefing requirements. Provide additional training.

## EXEMPLES D'OBSERVATIONS, DE LEÇONS IDENTIFIÉES ET DE RECOMMANDATIONS

Observation	Leçon identifiée	Recommandation
Les participants ont constaté que les suppléants ne recevaient pas un briefing complet lors de la passation de commandement.	Lorsque le commandement est transféré, le processus doit inclure un briefing qui saisit toutes les informations essentielles pour poursuivre des opérations sûres et efficaces, sinon les données seront perdues.	Revoir et formaliser le processus de transfert de commandement. Décrire les responsabilités du commandant de l'incident sortant et entrant et les exigences en matière d'exposé de la situation. Fournir une formation supplémentaire.



The core of the report will include a section for observations, lessons identified and recommendations for each objective. Quantitative information gathered through surveys and feedback forms is easily plugged into pie charts and graphs. Qualitative data should be molded into participant observations. It then falls on the expertise of the team to choose appropriate lessons and craft actionable recommendations.

### Observations

Observations come from participant experience during the exercise. These can be direct quotes, modified comments (especially where the original quote was unduly judgmental of a player or poorly written) or a compilation of comments from several sources. It is fully expected that players and other participants will identify anomalies in plan documentation and weakness in areas where additional training or awareness is required. Direct quotes should be directly attributed only to the facilitator or evaluator. Players should never be named directly or by function unless they have requested this. Instead, format observations as “a player observed ...” or “participants indicated ...”.

### Lessons Identified

Lessons identified should be connected directly to observations made by the participants. They are often pulled from industry best practices, standards or guidelines and are expressed as an adage.

### Recommendations

Recommendations should leverage the emergency or continuity management knowledge and experience of the report writer and evaluator(s). Recommendations outline activities that the organization can take to correct or strengthen plans, processes and procedures. Practically, each recommendation must begin with a verb and be actionable by the organization.

attirer l'attention des participants sur ce point. Beaucoup ne retourneront pas la page. Envisagez d'utiliser une couleur de papier vive et distincte pour les formulaires de feedback, comme le jaune ou l'orange. Cela permet d'éviter que les feuilles ne se perdent ou ne “sortent” de la salle.

## Créer un rapport remarquable

En concevant délibérément l'exercice pour atteindre les objectifs, l'équipe devrait avoir la tâche facile de rédiger un remarquable rapport après action. Le résumé devrait indiquer clairement si l'exercice a atteint chacun des objectifs. Il devrait présenter les preuves les plus solides que les ressources ont été bien utilisées pour l'exercice.

Le coeur du rapport comprendra une section pour les observations, les leçons identifiées et les recommandations pour chaque objectif. Les informations quantitatives recueillies par le biais d'enquêtes et de formulaires de retour d'information sont facilement intégrées dans des diagrammes circulaires et des graphiques. Les données qualitatives doivent être moulées dans les observations des participants. Il revient ensuite à l'expertise de l'équipe de choisir les leçons appropriées et d'élaborer des recommandations exploitables.

### Observations

Les observations proviennent de l'expérience des participants pendant l'exercice. Il peut s'agir de citations directes, de commentaires modifiés (surtout lorsque la citation originale portait un jugement excessif sur un joueur ou était mal rédigée) ou d'une compilation de commentaires provenant de plusieurs sources. On s'attend à ce que les joueurs et autres participants identifient des anomalies dans la documentation du plan et des faiblesses dans des domaines où une formation ou une sensibilisation supplémentaire est nécessaire. Les citations directes ne doivent être attribuées qu'à l'animateur ou à l'évaluateur. Les acteurs ne doivent jamais être nommés directement ou par fonction, sauf s'ils l'ont demandé. Formulez plutôt les observations en disant “un acteur a observé ...” ou “les participants ont indiqué ...”.

### Leçons identifiées

Les leçons identifiées doivent être directement liées aux observations faites par les participants. Ils sont souvent tirés des meilleures pratiques, normes ou directives du secteur et sont exprimés sous forme d'adage.

### Recommandations

Les recommandations doivent s'appuyer sur les connaissances et l'expérience en matière de gestion des situations d'urgence ou de continuité du rédacteur du rapport et du ou des évaluateurs. Les recommandations décrivent les activités que l'organisation peut entreprendre pour corriger ou renforcer les plans, processus et procédures. En pratique, chaque recommandation doit commencer par un verbe et être réalisable par l'organisation.

## Key Take Aways

1. Take the report into consideration from initial objective development through tool design and feedback collection.
2. Practice and invest time crafting exercise objectives that feed into the report.
3. Leverage instant and delayed feedback methods to maximize the value of the exercise.
4. Construct tools that embrace how different personality types communicate.
5. Practice transforming raw feedback into observations, lessons identified and recommendations.

Deploy deliberate design methods as they will lead to remarkable reports which dazzle senior management, shore up future funding and maximize the value of the exercise to your organization. ■

### References

- CSA Z1600-17 Emergency and continuity management program
- Disaster Recovery Institute International, The Professional Practices for Business Continuity Management, March 2017
- Handbook for developing public health emergency operations centre. Part C: training and exercises. World Health Organization 2018
- Handbook on evaluation of exercises. Karlstad: Swedish Civil Contingencies Agency (MSB); 2011
- ISO 22300, Societal security – Terminology
- ISO 22301, Societal security – Business continuity management systems – Requirements
- ISO 22320, Societal security – Emergency management – Requirements for incident response
- NFPA 1600, Standard for Disaster/Emergency Management Programs 2010 Edition
- U.S. Department of Homeland Security HSEEP (Homeland Security Exercise Evaluation Program): Volume I: HSEEP Overview and Exercise Programme Management; Volume II: Exercise Planning and Conduct; Volume III: Exercise Evaluation and Improvement Planning; Volume IV Library: Sample Exercise Materials.
- WHO simulation exercise manual. Geneva: World Health Organization; 2017.

## Principaux points à retenir

1. Tenez compte du rapport depuis l'élaboration de l'objectif initial jusqu'à la conception de l'outil et la collecte des commentaires.
2. Pratiquez et investissez du temps dans l'élaboration des objectifs de l'exercice qui alimentent le rapport.
3. Exploitez les méthodes de rétroaction instantanée et différée pour maximiser la valeur de l'exercice.
4. Construire des outils qui tiennent compte de la façon dont les différents types de personnalité communiquent.
5. S'entraîner à transformer le retour d'information brut en observations, leçons identifiées et recommandations.

Déployez des méthodes de conception délibérées, car elles conduiront à des rapports remarquables qui éblouiront les cadres supérieurs, consolideront les financements futurs et maximiseront la valeur de l'exercice pour votre organisation. ■

### Références

- CSA Z1600-17 Programme de gestion des urgences et de la continuité des activités
- Disaster Recovery Institute International, Les pratiques professionnelles pour la gestion de la continuité des activités, mars 2017.
- Manuel pour le développement d'un centre d'opérations d'urgence en santé publique. Partie C : formation et exercices. Organisation mondiale de la santé 2018
- Manuel d'évaluation des exercices. Karlstad : Agence suédoise pour les contingences civiles (MSB) ; 2011
- ISO 22300, Sécurité sociétale - Terminologie
- ISO 22301, Sécurité sociétale - Systèmes de management de la continuité d'activité - Exigences
- ISO 22320, Sécurité sociétale - Gestion des urgences - Exigences pour la réponse aux incidents.
- NFPA 1600, Norme pour les programmes de gestion des catastrophes/urgences, édition 2010
- Département de la sécurité intérieure des États-Unis HSEEP (Homeland Security Exercise Evaluation Program) : Volume I : Aperçu du HSEEP et gestion du programme d'exercices ; Volume II : Planification et exécution des exercices ; Volume III : Évaluation des exercices et planification des améliorations ; Volume IV Bibliothèque : Exemples de matériel d'exercice.
- Manuel d'exercices de simulation de l'OMS. Genève : Organisation mondiale de la santé ; 2017.

**Cynthia D. Wenn, MA CBCP CBCA CRM** is Vice President of Operations, Vanguard Emergency Management Consulting Inc.

Ms. Wenn graduated from York University, in Toronto, Ontario in 1999 with a Master of Arts degree. She spent several years underwriting a broad range of business risks for the Dominion of Canada and Lombard Insurance while obtaining her Certified Insurance Professional (CIP) and Canadian Risk Management (CRM) designation. In 2003, she joined Cognos Inc. advancing their risk management and business continuity initiatives. Since 2010, Cynthia has supported various projects at Vanguard EMC Inc., currently serving as Vice President of Operations. She has obtained the Certified Business Continuity Auditor (CBCA), the Certified Business Continuity Professional (CBCP) and the Incident Command 400 level designation. She sits on the Education Commission for DRI CANADA.



**Cynthia D. Wenn, MA CBCP CBCA CRM** est vice-présidente des opérations, Vanguard Emergency Management Consulting Inc.

Mme Wenn a obtenu une maîtrise ès arts de l'Université York, à Toronto, en Ontario, en 1999. Elle a passé plusieurs années à souscrire un large éventail de risques commerciaux pour le Dominion du Canada et Lombard Insurance, tout en obtenant le titre de Professionnelle d'assurance agréée (PAA) et de Gestion canadienne des risques (GCR). En 2003, elle s'est jointe à Cognos Inc. pour faire progresser leurs initiatives en matière de gestion des risques et de continuité des activités. Depuis 2010, Cynthia soutient divers projets chez Vanguard EMC Inc. et occupe actuellement le poste de vice-présidente des opérations. Elle a obtenu le titre d'auditeur certifié en continuité d'activité (CBCA), de professionnel certifié en continuité d'activité (CBCP) et le titre de commandant d'incident de niveau 400. Elle siège à la Commission de l'éducation de DRI CANADA.

# BCP in the Hybrid Working World

## BCP dans le monde du travail hybride

**By/Par Brenda Escribano, CBCP**

**S**o you think you have a Business Continuity Plan that is tried and true.... But the world has changed so quickly that it may no longer be relevant. Before the Covid-19 Pandemic we had “traditional” Business Continuity plans that had staff either going to their Work Area Recovery Premises or to Work from Home. Now that restrictions have eased and the world has shifted again, we have to face the new “normal” – hybrid work arrangements.

Countless organizations are in the process of reconsidering what their typical work environment looks like. We see new full time remote work, full time in the office and a blend of the two, which we like to refer to as the hybrid model. The hybrid model poses new and exciting opportunities for Business Continuity Professionals – and there are plenty of new risks that we need to be considering and contemplating on behalf of the businesses that we support.

For those of you who have not had experience with this new model, the hybrid work arrangement typically has people working in the office for a specific number of days per week and from their home offices the balance of the week. Any and all scenarios can exist – a one week on/off scenario to a few days per week in both the office and home office. Coupled with this change, a number of organizations are reducing their office footprint to reduce cost. What does that mean from a Business Continuity perspective? Let’s dive into that a little further. Let’s say your organization has 3 days in office and 2 days working from home arrangement. Desks in the office are at capacity each day and there are typically no extra desks available. What happens if there is a power outage that affects your staff working from home? You may have divested yourself of your recovery sites during the pandemic – where are these people going to go? How are you going to continue operations?

This scenario shows us how important it is to reconsider the old norms and work with today’s new normal. Business Continuity professionals need to now consider a whole host of new challenges. Do you displace non-critical staff in order to bring critical staff into the office? Do you need to encourage and espouse greater redundancy for employees as they work from home? If so, what does that mean from a bottom-line perspective? What human resources issues, if any, does this create for people who now have to go into the office, and what does that mean for those who are sent home to wait for the resolution of the incident?

This goes to show that in order to be resilient and to be prepared for the unexpected, organizations need trusted and trained Business Continuity professionals to help guide them through these unknown waters. As professionals, we not only know the important and relevant questions to ask, but we have quite possibly thought of both the solutions and potential pit falls already. ■

**Brenda Escribano, CBCP** is Associate Director, Business Continuity Management at RBC.



**Brenda Escribano, CBCP** est Associate Director, Business Continuity Management at RBC

**V**ous pensez donc avoir un plan de continuité des activités qui a fait ses preuves.... Mais le monde a changé si rapidement qu’il n’est peut-être plus pertinent. Avant la pandémie de Covid-19, nous avions des plans de continuité d’activité “traditionnels” dans lesquels le personnel se rendait dans les locaux de récupération de leur zone de travail ou travaillait à domicile. Maintenant que les restrictions se sont assouplies et que le monde a de nouveau changé, Nous devons faire face à la nouvelle “normalité” : les régimes de travail hybrides.

D’innombrables organisations sont en train de reconsidérer leur environnement de travail typique. Nous voyons de nouvelles formes de travail à distance à temps plein, à temps plein au bureau et un mélange des deux, que nous aimons appeler le modèle hybride. Le modèle hybride offre des opportunités nouvelles et passionnantes pour les professionnels de la continuité des activités - et il y a beaucoup de nouveaux risques que nous devons prendre en compte et envisager au nom des entreprises que nous soutenons.

Pour ceux d’entre vous qui n’ont pas encore fait l’expérience de ce nouveau modèle, le régime de travail hybride consiste généralement à travailler au bureau un certain nombre de jours par semaine et à domicile le reste de la semaine. Tous les scénarios sont possibles, qu’il s’agisse d’une semaine de travail ou de quelques jours par semaine au bureau et à domicile. Parallèlement à ce changement, un certain nombre d’organisations réduisent l’empreinte de leurs bureaux pour réduire les coûts. Qu’est-ce que cela signifie du point de vue de la continuité des activités ? Penchons-nous un peu plus sur la question. Supposons que votre organisation dispose de 3 jours au bureau et de 2 jours de travail à domicile. Les bureaux du bureau sont au maximum de leur capacité chaque jour et il n’y a généralement pas de bureaux supplémentaires disponibles. Que se passe-t-il si une panne de courant affecte votre personnel travaillant à domicile ? Vous vous êtes peut-être départi de vos sites de secours pendant la pandémie - où ces personnes vont-elles aller ? Comment allez-vous poursuivre vos opérations ?

Ce scénario nous montre combien il est important de reconsidérer les anciennes normes et de travailler avec la nouvelle normalité d’aujourd’hui. Les professionnels de la continuité des activités doivent désormais envisager toute une série de nouveaux défis. Devez-vous déplacer le personnel non critique afin de faire venir le personnel critique au bureau ? Devez-vous encourager et épouser une plus grande redondance des employés lorsqu’ils travaillent à domicile ? Si c’est le cas, qu’est-ce que cela signifie d’un point de vue financier ? Quels problèmes de ressources humaines, le cas échéant, cela crée-t-il pour les personnes qui doivent maintenant se rendre au bureau, et qu’est-ce que cela signifie pour ceux qui sont renvoyés chez eux pour attendre la résolution de l’incident ?

Cela montre que pour être résilientes et prêtes à faire face à l’inattendu, les organisations ont besoin de professionnels de la continuité d’activité fiables et formés pour les aider à traverser ces eaux inconnues. En tant que professionnels, nous connaissons non seulement les questions importantes et pertinentes à poser, mais nous avons probablement déjà pensé aux solutions et aux pièges potentiels. ■

# BIT Theory: Tracking Building Impacts during Business Continuity Incidents

## La théorie du BIT : Suivi des impacts sur les bâtiments pendant les incidents de continuité des activités

By/Par Paul Swanburg

**A** fundamental requirement for any incident response is maintaining situational awareness, which becomes challenging if the incident is affecting a large geographic area or several entities. Historically, determining impacts to workplaces and business activities has been a manual process that is heavily dependent on telecommunications, and with significant administrative overhead for “on the ground” personnel responding to the incident and those at the centralized emergency coordination center. There must be a better way.

The Nova Scotia provincial business continuity program embarked on an initiative codenamed Project LYCEUM to develop an innovative tool and data modelling that monitors, tracks and reports on workplace locations during disruptive incidents.

I was assigned to this project as a requirement of my work placement to complete the Emergency Management program at the Nova Scotia Community College (NSCC).

At its core, this innovative tool internally known as the Building Impact Tracker (BIT), combines two large databases and presents information in an easy to read and update format. The first database contains Business Impact Analysis information such as critical business functions and activities, recovery time objectives (RTO) and business impacts. The second database is a list of all workplaces and buildings the province monitors during incidents. These databases are maintained by provincial departments and updated frequently.

BIT has been successfully piloted in real incidents such as the recent New Brunswick/Nova Scotia border blockade, active shooter incidents and single building incidents.

Project Lyceum was a great experience for me and I'm happy to have been a part of it. It gave me a more nuanced view of Business Continuity as opposed to the “by the book” viewpoint that comes in an academic setting. Seeing things like RTO/MTPD/BCMO embedded into a larger organization and the emphasis on infrastructure has expanded my understanding of business continuity planning greatly.

**U**ne exigence fondamentale pour toute réponse à un incident est le maintien de la connaissance de la situation, ce qui devient un défi si l'incident affecte une grande zone géographique ou plusieurs entités. Historiquement, la détermination des impacts sur les lieux de travail et les activités commerciales a toujours été un processus manuel, fortement dépendant des télécommunications et entraînant des frais administratifs importants pour le personnel “sur le terrain” qui répond à l'incident et pour celui du centre de coordination des urgences. Il doit y avoir une meilleure solution.

Le programme provincial de continuité des activités de la Nouvelle-Écosse s'est lancé dans une initiative portant le nom de code “Projet LYCEUM” afin de développer un outil innovant et une modélisation des données permettant de surveiller, de suivre et de rendre compte des lieux de travail lors d'incidents perturbateurs.

J'ai été assigné à ce projet dans le cadre de mon stage de travail pour compléter le programme de gestion des urgences au Nova Scotia Community College (NSCC).

Cet outil innovant, connu en interne sous le nom de Building Impact Tracker (BIT), combine deux grandes bases de données et présente les informations dans un format facile à lire et à mettre à jour. La première base de données contient des informations sur l'analyse de l'impact sur les entreprises, telles que les fonctions et activités essentielles, les objectifs de temps de récupération (RTO) et les impacts sur les entreprises. La deuxième base de données est une liste de tous les lieux de travail et bâtiments que la province surveille pendant les incidents. Ces bases de données sont maintenues par les ministères provinciaux et mises à jour fréquemment.

La théorie TBI relie l'état de chaque lieu de travail avec les données critiques liées à la continuité des activités pour ce lieu, tandis que les planificateurs de la continuité des activités peuvent tirer des rapports précis et en temps réel à partager avec la direction générale pour une prise de décision rapide. La théorie TBI pour faciliter la collecte et le partage des données est largement applicable pour les impacts géographiques massifs tels que les coupures de courant après une tempête, ou pour un incident sur

I thank you for taking the time to read this article and hopefully your knowledge has been expanded with the description of the thought process behind the BIT theory.

The BIT theory links the status of each workplace location with critical business continuity related data for that location, whilst Business Continuity Planners can pull accurate and real time reports to share with Senior Leadership for timely decision making. The BIT theory for facilitating data collection and sharing has broad applicability for mass geographic impacts such as power outages following a storm, or for a single location incident that partially or entirely affects a workplace such as a building fire, or for a mass emergency situation such as an active shooter or COVID-19 community exposure.

Guiding principles for BIT theory were developed from lessons learned in previous incidents, the primary principle being that information should be easy to capture and maintain during incidents. More data points meant exponential effort to update the data which is difficult to do during incidents.

Additional principles include that BIT theory should follow established business continuity best practices, and source data from a mix of dynamic and semi-dynamic data sets as follows:

**Dynamic data** – provided by Incident Commanders

- Impacts to safety and business operations.
- Progress on activating business continuity plans (includes employees unable to work remotely).

un seul site qui affecte partiellement ou entièrement un lieu de travail tel qu'un incendie de bâtiment, ou pour une situation d'urgence massive telle qu'un tireur actif ou une exposition de la communauté COVID-19.

Les principes directeurs de la théorie TBI ont été élaborés à partir des leçons tirées d'incidents précédents, le principe principal étant que les informations doivent être faciles à saisir et à conserver pendant les incidents. Plus de points de données signifie un effort exponentiel pour mettre à jour les données, ce qui est difficile à faire pendant les incidents.

D'autres principes prévoient que la théorie TIB doit suivre les meilleures pratiques établies en matière de continuité des activités et qu'elle doit s'appuyer sur des données provenant d'une combinaison de jeux de données dynamiques et semi-dynamiques, comme suit :

**Données dynamiques** - fournies par les commandants d'incidents

- Impacts sur la sécurité et les opérations commerciales.
- Progrès dans l'activation des plans de continuité des activités (y compris les employés qui ne peuvent pas travailler à distance).
- Statut du bâtiment/lieu de travail affecté.
- Temps de restauration prévu.
- Mise à jour de l'avancement des réparations.

**Données semi-dynamiques** - maintenues par le programme provincial de continuité des affaires (analyse de l'impact sur les affaires)

Datapoint	Purpose	Objectif
ID	A unique identifier to link a workplace building to critical business functions.	Un identifiant unique permettant de relier un bâtiment de travail à des fonctions commerciales essentielles.
Building Status / État du bâtiment	To determine the accessibility and operational capability of the building.	Déterminer l'accessibilité et la capacité opérationnelle du bâtiment.
Tenants / Locataires	To determine all department that have a presence in the building	Déterminer tous les départements qui ont une présence dans le bâtiment.
Building Name & Address / Nom et adresse du bâtiment	To determine the address of the building for reference and geo-mapping purposes.	Pour déterminer l'adresse du bâtiment à des fins de référence et de géocartographie
Building Category / Catégorie de bâtiment	Provides details about the type and level of access for the building include Public Facing, Non Public Facing, Hybrid, Warehouse, Critical Infrastructure.	Fournit des détails sur le type et le niveau d'accès du bâtiment, notamment face au public, face au non public, hybride, entrepôt, infrastructure critique.
Building Impacts / Impacts sur les bâtiments	Includes criteria for restoration times within RTO; Service Level below acceptable thresholds; Safety hazards affecting employees and clients; impacts to operations and assets.	Comprend des critères pour les délais de rétablissement dans le cadre de la RTO ; le niveau de service en dessous des seuils acceptables ; les risques pour la sécurité des employés et des clients ; les impacts sur les opérations et les actifs.
Damage Summary / Résumé des dommages	Provides a summary of impacts to the building such as Active Shooter, Fire, Flood, Power Outage, Parking Lot in-accessible (Snowstorms), Pandemic Exposure and Structural Impacts.	Fournit un résumé des impacts sur le bâtiment tels que Fusillade active, incendie, inondation, panne de courant, parking inaccessible (tempêtes de neige), exposition à une pandémie et impacts structurels.
Damage Report / Rapport sur les dommages	Provides details regarding the impacts to the building.	Fournit des détails concernant les impacts sur le bâtiment.
Expected Restoration Time / Temps de restauration prévu	Provides an estimate of when the workplace is expected to become operational.	Fournit une estimation de la date à laquelle le lieu de travail devrait devenir opérationnel.
Critical Business Functions / Fonctions commerciales essentielles	Provides overall priority of critical business functions based on time (RTO) and severity. This helps prioritize critical business functions during a disruption.	Fournit la priorité globale des fonctions commerciales critiques en fonction du temps (RTO) et de la gravité. Cela permet de hiérarchiser les fonctions critiques de l'entreprise pendant une perturbation.

- Status of affected building/workplace.
- Expected Restoration Time.
- Repair progress updates.

**Semi-Dynamic data** – maintained by provincial Business Continuity Program (Business Impact Analysis)

- Critical business functions and activities operating in the building/workplace including RTO, severity and risk related data.
- Building Name and Address.
- Building Category (public facing, warehouse, critical infrastructure etc.)
- Building Lead Contact.
- An approximate number of employees and visitors during normal operations.

I developed the framework for the BIT tool, making extensive use of the Power Automate function using Microsoft Sharepoint and Microsoft Teams to “flow” the data between different data points. If you wanted to employ BIT theory on a smaller scale and did not already have the digital infrastructure, then BIT could serve as both building list and a critical business function list in an Excel spreadsheet format.

BIT has been successfully piloted in real incidents such as the recent New Brunswick/Nova Scotia border blockade, active shooter incidents and single building incidents.

Project Lyceum was a great experience for me and I’m happy to have been a part of it. It gave me a more nuanced view of Business Continuity as opposed to the “by the book” viewpoint that comes in an academic setting. Seeing things like RTO/MTPD/BCMO embedded into a larger organization and the emphasis on infrastructure has expanded my understanding of business continuity planning greatly. I thank you for taking the time to read this article and hopefully your knowledge has been expanded with the description of the thought process behind the BIT theory. ■

- Fonctions et activités commerciales critiques opérant dans le bâtiment/le lieu de travail, y compris les données relatives au RTO, à la gravité et aux risques.
- Nom et adresse du bâtiment.
- Catégorie de bâtiment (public, entrepôt, infrastructure critique, etc.)
- Contact principal du bâtiment.
- Le nombre approximatif d’employés et de visiteurs pendant les opérations normales.

J’ai développé le cadre de l’outil TIB, en faisant un usage intensif de la fonction Power Automate en utilisant Microsoft Sharepoint et Microsoft Teams pour “faire circuler” les données entre les différents points de données. Si vous vouliez employer la théorie TIB à plus petite échelle et que vous ne disposiez pas déjà de l’infrastructure numérique, alors la TIB pourrait servir à la fois de liste de construction et de liste des fonctions critiques de l’entreprise dans un format de feuille de calcul Excel..

Le TBI a été mis à l’essai avec succès dans le cadre d’incidents réels tels que le récent blocus de la frontière entre le Nouveau-Brunswick et la Nouvelle-Écosse, des incidents de tir actif et des incidents touchant un seul bâtiment.

Le projet Lyceum a été une grande expérience pour moi et je suis heureux d’en avoir fait partie. Il m’a permis d’avoir une vision plus nuancée de la continuité des activités, par opposition au point de vue “théorique” que l’on trouve dans un cadre universitaire. Le fait de voir des éléments tels que RTO/MTPD/BCMO intégrés dans une organisation plus vaste et l’accent mis sur l’infrastructure ont considérablement élargi ma compréhension de la planification de la continuité des activités. Je vous remercie d’avoir pris le temps de lire cet article et j’espère que la description du processus de réflexion qui sous-tend la théorie du TBI a élargi vos connaissances. ■

**Paul Swanburg, BAH**

*is an officer in the Canadian Armed Forces as well as the owner/operator of Stratagem Business Continuity Solutions, an independent, small business-oriented consulting firm in the Annapolis Valley, N.S.*

*A graduate of Acadia University with a B.A. in Politics and Nova Scotia Community College with an Advanced Diploma in Emergency Management, Paul has established himself early on with his creation of the Building Impact Tracker for the Province of Nova Scotia and independent plans for small business in the local area.*

*Paul is a proud volunteer with his local Fire Department; in his spare time he enjoys keeping informed of current issues, and maintaining his skills through independent study.*



**Paul Swanburg, BAH**

*est officier dans les Forces armées canadiennes et propriétaire-exploitant de Stratagem Business Continuity Solutions, une société d’experts-conseils indépendante axée sur les petites entreprises située dans la vallée de l’Annapolis, en Nouvelle-Écosse.*

*Diplômé de l’Université Acadia avec un baccalauréat en politique et du Nova Scotia Community College avec un diplôme avancé en gestion des urgences, Paul s’est établi très tôt avec la création du Building Impact Tracker pour la province de la Nouvelle-Écosse et des plans indépendants pour les petites entreprises de la région.*

*Paul est un fier bénévole de son service d’incendie local; dans ses temps libres, il aime se tenir au courant des questions d’actualité et maintenir ses compétences grâce à des études indépendantes.*

# Project Managing a Business Continuity and Disaster Recovery Program Build

## Gestion de projet pour la construction d'un programme de continuité des activités et de reprise après sinistre

By/Par Sukhmani Sandhu, PMP



**B**usiness Continuity and Disaster Recovery planning (BC & DRP) is crucial for all organizations whether it be public or private sector, yet it is often not a priority amongst the list of active projects. It loops in Emergency Management Planning, Enterprise/Operational Risk Management Planning, Occupational Health & Safety, Cyber Security/Data Protection, and Privacy if done correctly, but paying big bucks at the time of crises appears to be the trend. As a famous saying goes; “5 extra minutes spent in the beginning can save you 500 plus hours at the end.” A similar concept applies in prioritizing BCDR for the growth and nurturing of organizational assets. It should by default, be part of the organization’s objectives.

From a project management perspective, a licensed and experienced driver should drive the bus with the right folks seated on the correct seats, and individuals must be dropped off at a precise location to on-board more, if required. To begin the BCDR program build, a certified business continuity professional (ABCP, CBCP, or MBCP), as the subject matter expert, should be assigned as the project lead. This individual or team, working with the project manager and business analyst, will define current and future state to produce a gap analysis and proceed from there. Since this initiative is organization wide, the

**L**a planification de la continuité des activités et de la reprise après sinistre (BC & DRP) est cruciale pour toutes les organisations, qu’il s’agisse du secteur public ou du secteur privé, mais elle n’est souvent pas une priorité dans la liste des projets actifs. Si elle est correctement réalisée, elle s’intègre parfaitement à la planification de la gestion des urgences, à la planification de la gestion des risques d’entreprise/opérationnels, à la santé et à la sécurité au travail, à la cybersécurité/protection des données et à la protection de la vie privée, mais la tendance semble être de verser des sommes importantes au moment des crises. Comme le dit un célèbre proverbe, “5 minutes supplémentaires passées au début peuvent vous faire gagner 500 heures et plus à la fin”. “Un concept similaire s’applique à l’établissement de priorités en matière de BCDR pour la croissance et le développement des actifs organisationnels. Elle devrait, par défaut, faire partie des objectifs de l’organisation.

Du point de vue de la gestion de projet, un chauffeur expérimenté et titulaire d’un permis doit conduire l’autobus avec les bonnes personnes assises sur les bons sièges, et les personnes doivent être déposées à un endroit précis pour en embarquer d’autres, si nécessaire. Pour commencer l’élaboration du programme BCDR, un professionnel certifié en continuité des affaires (ABCP, CBCP ou MBCP), en tant qu’expert en la matière, doit être désigné comme chef de projet. Cette personne ou cette équipe, en collaboration avec le chef de projet et l’analyste d’affaires, définira l’état actuel et futur afin de produire une analyse des lacunes et de procéder à partir de là. Étant donné que cette initiative concerne l’ensemble de l’organisation, les représentants et les experts en la matière (PME) de toutes les disciplines de l’entreprise doivent travailler ensemble. Ni l’infrastructure informatique, ni aucun autre département (finances, marketing, opérations, etc.) ne peut faire quoi que ce soit tout seul, il doit s’agir d’une initiative d’équipe à l’échelle de l’organisation.

representatives and subject matter experts (SMEs) from all disciplines of the business must work together. Neither IT Infrastructure, nor any other department (finance, marketing, operations, etc.) can do anything alone, it must be an organization-wide, team initiative.

A common misconception (or delusion) is that IT can fix everything and knows the functioning or dependencies of the business. The reality is that IT folks often don't fully absorb the concept of BCDR, what is asked or requested of them, and how this initiative will help make their job relatively easy during a crisis or unplanned operational outages. With a plan in place, the right people will be contacted and will work towards the solution, as opposed to not having a plan, the right people with clarity on what has occurred, how a crisis is developing, and what to do next to control the damage in dollars, customer connections, and partner relations.

BCDR is not a small undertaking which can be completed in few months in a medium to large organization. Depending on the size and complexity of the business, the number of BCDR professionals in the group, and experience of the business SMEs, building a BCDR Program can run for up to 3-5 years and is a living process that must always be maintained. Having the right people at right time has been emphasized over and over because it is something that can determine the success and failure of the initiative. The BCDR process in some organizations might be considered done once the program is built, but, it will become stale very quickly if expertise and experience in BCDR is not kept in house. The documents prepared and findings from this process must be revisited and updated to maintain the viability and authenticity of the mitigation plans. If you are doing this first time, don't be afraid or feel shy about seeking out expert advice from the market. It is better to be done correctly the first time than reinvesting the resources and effort in correcting it. ■

Une idée fausse courante (ou une illusion) est que l'informatique peut tout régler et qu'elle connaît le fonctionnement ou les dépendances de l'entreprise. En réalité, les informaticiens n'assimilent souvent pas complètement le concept de BCDR, ce qu'on leur demande ou ce qu'on attend d'eux, et comment cette initiative leur facilitera relativement la tâche en cas de crise ou d'interruptions opérationnelles imprévues. Avec un plan en place, les bonnes personnes seront contactées et travailleront à la solution, alors qu'en l'absence de plan, les bonnes personnes auront une idée claire de ce qui s'est passé, de l'évolution de la crise et des mesures à prendre pour limiter les dégâts en termes d'argent, de relations avec les clients et de relations avec les partenaires.

Le programme BCDR n'est pas une petite entreprise qui peut être menée à bien en quelques mois dans une organisation de taille moyenne ou grande. Selon la taille et la complexité de l'entreprise, le nombre de professionnels du BCDR dans le groupe et l'expérience des PME de l'entreprise, la mise en place d'un programme de BCDR peut durer jusqu'à 3 à 5 ans et constitue un processus vivant qui doit toujours être maintenu. La nécessité de disposer des bonnes personnes au bon moment a été soulignée à maintes reprises, car c'est un élément qui peut déterminer le succès ou l'échec de l'initiative. Dans certains organismes, on peut considérer que le processus de RADC est terminé une fois le programme mis en place, mais il se périmerait très rapidement si l'expertise et l'expérience en RADC ne sont pas conservées en interne. Les documents préparés et les conclusions de ce processus doivent être revus et mis à jour pour maintenir la viabilité et l'authenticité des plans d'atténuation. Si vous faites cela pour la première fois, n'ayez pas peur ou ne soyez pas gêné de demander des conseils d'experts sur le marché. Il vaut mieux faire les choses correctement dès la première fois que de réinvestir les ressources et les efforts pour les corriger. ■

### **Sukhmani Sandhu, PMP**

*is a licensed project manager and has experience working on Infrastructure and Application Management projects in both public and private sector. She enjoys the project management side of the world and in parallel wants to building expertise in change management and negotiation strategies, something that intrigues her. She believes in giving back to the community and does not miss any opportunity she is offered to work and volunteer with the community. Outside work, she enjoys hiking, kayaking, target shooting, exploring, and being close to nature. On the adventure side, she has done skydiving, bungee jumping, white water rafting, and is now working towards becoming a scuba diver.*



### **Sukhmani Sandhu, PMP**

*est une gestionnaire de projet agréée et a de l'expérience dans les projets de gestion d'infrastructure et d'application dans les secteurs public et privé. Elle aime le côté gestion de projets et souhaite parallèlement acquérir une expertise en gestion du changement et en stratégies de négociation, ce qui l'intrigue. Elle croit en la nécessité de redonner à la communauté et ne manque aucune occasion qui lui est offerte de travailler et de faire du bénévolat au sein de la communauté. En dehors du travail, elle aime la randonnée, le kayak, le tir à la cible, l'exploration et être proche de la nature. Pour ce qui est de l'aventure, elle a fait du parachutisme, du saut à l'élastique, du rafting en eaux vives et travaille actuellement à devenir plongeuse sous-marine.*

# OUT WITH THE “OLD” AND IN WITH THE “NEW” Moving Beyond Business Continuity!

By/Par Reta Setrak, MBCP

**Y**es. Business Continuity is the “OLD”. If your organization still operates within those parameters, be ready to continuously fall short of C-suite expectations, prove your worth, and beg for support.

So, what is the “new” you may ask? **RESILIENCE!** Yes, yes, I know this is not new... everyone has been preaching resilience for years but what does it really mean to you?

# LE “VIEUX” S’EN VA ET LE “NOUVEAU” ARRIVE Aller au-delà de la continuité des activités!

**O**ui, la continuité des activités est l’“OLD”. Si votre organisation fonctionne toujours selon ces paramètres, soyez prêt à ne jamais répondre aux attentes de la direction, à prouver votre valeur et à mendier votre soutien.

Alors, quelle est la “nouveau”, me direz-vous ?  
**LA RÉSILIENCE !** Oui, oui, je sais que ce n’est pas nouveau... tout le monde prêche la résilience depuis des années, mais qu’est-ce que cela signifie vraiment pour vous ?



What Have  
You Learned?

I have been researching, experimenting, and testing what resilience means in an organization. Although, you will find many different definitions, I was able to narrow it down to one: “moving from being reactive into becoming proactive”. This is based on learnings and real-life experiences.

Let me take you back to where I learned, at a very young age, what it means to survive a crisis and be resilient. I was born in Baghdad, the largest city in the now war-torn Iraq. In August of 1990, Iraq invaded neighboring Kuwait, months later, in January 1991, an international coalition began extensive aerial bombing of the invading country. Laser-targeted missiles became the main weapon of choice for coalition forces, here, the importance of planning and being prepared was clear.

When you face events that are more significant than you are, where the unknown is greater than what you can imagine, you must have plans, tools, and a way to absorb the impact while limiting your losses. For me, digging and using an underground bunker in the front yard and stocking up on food and fuel became part of normal, daily life. Our day-to-day functions had to adjust to be in line with the day's circumstances. Is the water running? Is the electricity on? How much food is left? What can you give up today so you can save for tomorrow?

These experiences helped me learn the importance of planning. It showed me that making sure you are prepared before a crisis occurs, can limit its impact, and therefore allow you to operate at a meaningful level in the hardest of times.

In short, building backups and testing them once a year is no longer enough. Passing the buck to the technology teams to build IT Disaster Recovery and stand at an arms length is also no longer enough. Saying that emergency response and physical security can live under facilities or security and that “it's not my problem” is no longer feasible. Building recovery strategies after key operational decisions and business planning has been completed is no longer acceptable.

So how do you achieve resilience?

- Build a holistic program
- Build operational redundancy
- Do not let a good crisis go to waste!

**Building a holistic program** with Emergency Response, Crisis Management, Business Continuity, and IT Disaster Recovery Oversight, is the way to go. Connecting the dots between security events, personnel crises, cyber incidents, key third party outages and even with a good old flood and fire, is how your program should operate.

J'ai cherché, expérimenté et testé ce que signifie la résilience dans une organisation. Bien que vous trouviez de nombreuses définitions différentes, j'ai réussi à en réduire le nombre à une seule : “passer d'une situation réactive à une situation proactive”. Cette définition est basée sur des apprentissages et des expériences réelles.

Permettez-moi de vous ramener à l'endroit où j'ai appris, à un très jeune âge, ce que signifie survivre à une crise et être résilient. Je suis né à Bagdad, la plus grande ville de l'Irak, aujourd'hui déchirée par la guerre. En août 1990, l'Irak a envahi le Koweït voisin. Quelques mois plus tard, en janvier 1991, une coalition internationale a commencé à bombarder massivement le pays envahi. Les missiles à visée laser sont devenus l'arme principale des forces de la coalition. L'importance de la planification et de la préparation est alors évidente.

Lorsque vous êtes confronté à des événements plus importants que vous, où l'inconnu est plus grand que ce que vous pouvez imaginer, vous devez avoir des plans, des outils et un moyen d'absorber l'impact tout en limitant vos pertes. Pour moi, le fait de creuser et d'utiliser un bunker souterrain dans la cour avant et de faire des réserves de nourriture et de carburant est devenu une partie de la vie normale et quotidienne. Nos fonctions quotidiennes ont dû s'adapter aux circonstances du jour. L'eau coule-t-elle ? L'électricité est-elle allumée ? Combien de nourriture reste-t-il ? À quoi pouvez-vous renoncer aujourd'hui pour économiser pour demain ?

Ces expériences m'ont permis d'apprendre l'importance de la planification. Elles m'ont montré que le fait de s'assurer que l'on est préparé avant qu'une crise ne survienne peut en limiter l'impact et, par conséquent, vous permettre de fonctionner à un niveau significatif dans les moments les plus difficiles.

En bref, il ne suffit plus de créer des sauvegardes et de les tester une fois par an. Il ne suffit plus non plus de renvoyer la balle aux équipes technologiques pour qu'elles mettent en place une reprise après sinistre et se tiennent à distance. Dire que les interventions d'urgence et la sécurité physique peuvent relever des installations ou de la sécurité et que “ce n'est pas mon problème” n'est plus possible. Il n'est plus acceptable d'élaborer des stratégies de reprise après la prise de décisions opérationnelles clés et la planification des activités.

Alors comment atteindre la résilience ?

- Construire un programme holistique
- Construire une redondance opérationnelle
- Ne laissez pas une bonne crise se perdre !

**L'élaboration d'un programme holistique** comprenant la réponse aux urgences, la gestion de crise, la continuité des activités et la supervision de la reprise après sinistre informatique est la voie à suivre. Votre programme doit fonctionner en reliant les événements de sécurité, les crises du personnel, les cyberincidents, les pannes de tiers et même les bonnes vieilles inondations et les incendies.

Applying a risk lens with the 3-lines of defense approach also allows you to build appropriate accountabilities with proper oversight.

Let us dissect that a bit. As resilience professionals, we must clearly define our role as the second line defense. While physical security, facilities, technology, and the business own the plans and the tools; we are the ones that have the oversight, coordination, and ability to question the first line on the adequacy of their plans, tools, and guidelines, through rigorous testing and exercises.

If we take ownership of what is not ours, we will quickly fall into the old way of doing business continuity planning, where we knock on doors once a year and beg for some attention.

**Build operational redundancy** by being part of key operational decisions and apply the resilience view to essential planning. Think beyond technology redundancy. Ask yourself, where do we build the next location? How do we split work across regions? How do we build redundancy in our supply chain? How do we build redundancy in knowledge and business insight? How does hybrid work fit into all this? Then, adopt the technology that is flexible and more resilient in its operations.

**Do not let a good crisis go to waste!** Let's admit it, the pandemic was good for our business as resilience professionals. It forced organizations to adopt more flexible work practices, better technology, and fewer site and physical dependencies. In 2019, only fax and fresh signatures were acceptable, now we have turned to more digital and virtual options. The pandemic was, and still is, a turning point for every resilience professional, we are no longer only applicable if there is a flood, fire, or a big storm. This global event, in addition to the heightened cyber security risks, opened everyone's eyes to the diversity of skills we bring and the importance of what we do. Do not let it go to waste. Build on the momentum, keep reminding people of it, and use every incident to build better and more resilient programs that can withstand the next event. ■

**Reta Setrak, MBCP**  
Director Enterprise  
Risk & Resilience  
Canada Pension Plan  
Investment Board.

*Reta manages a  
Global Resiliency  
Program with direct  
responsibility for sites  
in Canada, USA, Asia,  
India, Australia, Brazil  
and China.*



L'application d'une lentille de risque avec l'approche des 3 lignes de défense vous permet également d'établir des responsabilités appropriées avec une supervision adéquate.

Disséquons un peu cela. En tant que professionnels de la résilience, nous devons clairement définir notre rôle de défense de deuxième ligne. Alors que la sécurité physique, les installations, la technologie et l'entreprise possèdent les plans et les outils, nous sommes ceux qui ont la supervision, la coordination et la capacité de questionner la première ligne sur l'adéquation de leurs plans, outils et directives, à travers des tests et exercices rigoureux.

Si nous nous approprions ce qui ne nous appartient pas, nous retomberons rapidement dans l'ancienne méthode de planification de la continuité des activités, qui consiste à frapper aux portes une fois par an pour quémander un peu d'attention.

**Créez une redondance opérationnelle** en prenant part aux décisions opérationnelles clés et en appliquant la perspective de la résilience à la planification essentielle. Pensez au-delà de la redondance technologique. Posez-vous la question suivante : où construire le prochain site ? Comment répartir le travail entre les régions ? Comment créer une redondance dans notre chaîne d'approvisionnement ? Comment créer une redondance dans la connaissance et la compréhension des affaires ? Comment le travail hybride s'intègre-t-il dans tout cela ? Ensuite, adoptez la technologie la plus souple et la plus résiliente dans ses opérations.

**Ne laissez pas une bonne crise se perdre !** Admettons-le, la pandémie a été bénéfique pour nos activités de professionnels de la résilience. Elle a forcé les organisations à adopter des pratiques de travail plus flexibles, une meilleure technologie et moins de dépendances de sites et physiques. En 2019, seuls le fax et les signatures fraîches étaient acceptables, maintenant nous nous sommes tournés vers des options plus numériques et virtuelles. La pandémie a été, et est toujours, un tournant pour chaque professionnel de la résilience, nous ne sommes plus seulement applicables en cas d'inondation, d'incendie ou de grosse tempête. Cet événement mondial, en plus des risques accrus de cybersécurité, a ouvert les yeux de tous sur la diversité des compétences que nous apportons et l'importance de ce que nous faisons. Ne laissez pas tout cela se perdre. Continuez sur votre lancée, rappelez-le sans cesse aux gens et utilisez chaque incident pour bâtir des programmes meilleurs et plus résilients, capables de résister au prochain événement. ■

**Reta Setrak, MBCP**  
Directeur des risques et de la résilience de l'entreprise  
Office d'investissement du régime de pensions du Canada.

*Reta gère un programme de résilience mondiale avec la responsabilité directe de sites au Canada, aux États-Unis, en Asie, en Inde, en Australie, au Brésil et en Chine.*

# Business Continuity Planning for the Remote Worker

## Planification de la continuité des activités pour le travailleur à distance

By/Par Vito Mangialardi, CBCP  
Business Continuity @ Metrolinx



**P**art of business continuity planning for any organization should include ensuring the ability of the organization to continue to function with minimum disruption after a severe outage, emergency, or disaster. This extends to those employees working remotely at home.

The remote worker, also known as the telework experience, has evolved since COVID-19 entered in 2020. Many surveys have indicated staff is more productive working from home than in the office. This is due to improved work-life balance with flexible working schedules, hybrid models splitting time between the home office and the workplace, and how and when we must commute to the office.

**D**ans le cadre de la planification de la continuité des activités de toute organisation, il convient de s'assurer de la capacité de l'organisation à continuer à fonctionner avec un minimum de perturbations après une panne, une urgence ou une catastrophe grave. Cela s'applique également aux employés qui travaillent à distance, chez eux.

Le travailleur à distance, également connu sous le nom de télétravail, a évolué depuis l'arrivée de COVID-19 en 2020. De nombreuses enquêtes ont indiqué que le personnel est plus productif en travaillant à domicile qu'au bureau. Cela est dû à l'amélioration de l'équilibre entre vie professionnelle et vie privée grâce à des horaires de travail flexibles, à des modèles hybrides partageant le temps entre le bureau à domicile et le lieu de travail, et à la manière et au moment où nous devons nous rendre au bureau.

Wikipedia defines telecommuting as remote work or telework as an arrangement in which employees do not commute to a central place of work. A person who telecommutes is known as a “telecommuter,” “teleworker,” and sometimes as a “home-sourced” employee. Many telecommuters work from home, while others, called “nomad workers,” use mobile telecommunications technology to work from coffee shops or other locations. This is a very familiar term because of the lengthy COVID-19 pandemic.

COVID-19 has significantly altered how we think about work, where we work, and the employee who does the work. Even the word ‘workplace’ has changed to mean anywhere, including our favorite coffee shop. COVID-19 and other past events have proven to be a platform for change at lightning speed. The experience gained during this pandemic has revealed both opportunities and challenges to the future of work.

Introducing teleworkers into the workplace for business continuity has many benefits and has been around long before the COVID-19 pandemic. For example, a risk mitigation strategy for staff who execute key processes is to redistribute or partition your workforce into multiple locations. If one workplace has operational issues, the other remains fully functional. An excellent example was used during SARS, whereby separating staff reduced the risk of many catching the virus. This would have resulted in greater absenteeism numbers from the office and greater overall numbers.

Regardless of whether business operations are conducted from an office tower (central place of work) or executed from home (where the employee lives), business continuity planning should be addressed as unfortunate incidents (disasters /emergencies/outages) can occur anywhere and cause a period of total or partial interruption to normal business operations. An incident could be a fire, flood, furnace explosion, or a much less dramatic event such as loss of electric power, cell, or internet service. Even short interruptions can have a significant effect on business. They can result in the loss of essential data or business records which can impair the delivery of your products and services and result in brand or reputational damage and dissatisfied customers.

Although developing a business continuity plan can be time-consuming, it should be considered an investment rather than an expense. In the long term, an effective business continuity plan can support an organization to become a differentiator from its competitors and save significant money, time, and emotional stress.

Senior management must support the development of the business continuity plan for supporting enterprise-wide remote work policy. Managers responsible for teleworking employees should be directly involved in preparing a plan

Wikipedia définit le télétravail comme un travail à distance ou le télétravail comme un arrangement dans lequel les employés ne se rendent pas à un lieu de travail central. Une personne qui fait du télétravail est connue sous le nom de “ télétravailleur “ , “ télétravailleur “ , et parfois comme un employé “ à domicile “. De nombreux télétravailleurs travaillent à domicile, tandis que d’autres, appelés “travailleurs nomades”, utilisent la technologie des télécommunications mobiles pour travailler depuis des cafés ou d’autres lieux. Ce terme est très familier en raison de la longue pandémie de COVID-19.

COVID-19 a considérablement modifié la façon dont nous concevons le travail, le lieu où nous travaillons et l’employé qui effectue le travail. Même le mot “lieu de travail “ a changé pour signifier n’importe où, y compris notre café préféré. COVID-19 et d’autres événements passés ont prouvé qu’ils constituaient une plate-forme de changement à la vitesse de l’éclair. L’expérience acquise au cours de cette pandémie a révélé à la fois des opportunités et des défis pour l’avenir du travail.

L’introduction de télétravailleurs sur le lieu de travail pour assurer la continuité des activités présente de nombreux avantages et existait déjà bien avant la pandémie de COVID-19. Par exemple, une stratégie d’atténuation des risques pour le personnel qui exécute des processus clés consiste à redistribuer ou à répartir vos effectifs sur plusieurs sites. Si un lieu de travail connaît des problèmes opérationnels, l’autre reste pleinement fonctionnel. Un excellent exemple a été utilisé pendant le SRAS, où la séparation du personnel a réduit le risque que beaucoup d’entre eux attrapent le virus. Cela aurait entraîné un taux d’absentéisme plus élevé au bureau et des chiffres globaux plus importants.

Que les opérations commerciales soient menées à partir d’une tour de bureaux (lieu de travail central) ou exécutées à domicile (là où vit l’employé), la planification de la continuité des activités doit être abordée car des incidents malheureux (catastrophes / urgences / pannes) peuvent se produire n’importe où et provoquer une période d’interruption totale ou partielle des opérations commerciales normales. Il peut s’agir d’un incendie, d’une inondation, d’une explosion de fourneau ou d’un événement beaucoup moins dramatique comme la perte de l’alimentation électrique, du service de téléphonie mobile ou d’Internet. Même de courtes interruptions peuvent avoir un effet important sur les affaires. Elles peuvent entraîner la perte de données essentielles ou d’enregistrements commerciaux, ce qui peut nuire à la fourniture de vos produits et services et entraîner une atteinte à la marque ou à la réputation et le mécontentement des clients.

Bien que l’élaboration d’un plan de continuité des activités puisse prendre du temps, elle doit être considérée comme un investissement plutôt que comme une dépense.



as they are intimately familiar with the operations and functions of the organization and are most likely to be aware of any weaknesses or vulnerabilities.

The first step in developing a business continuity plan is to define and inventory the business processes that will be/currently executed from the home office and understand their relative importance to other work functions and/or activities within the output (deliverable) supports. The next step is to determine the criticality of each business process and which needs to be preserved and remain operational without disruption as they are essential to business operations or revenue.

Once the criticality of the business processes is established, including the required infrastructure, the areas of risk exposure to the business need to be determined. A high-level risk assessment should be conducted to identify the points of most significant risk and impacts on business output and revenue. Problem scenarios should be analyzed to determine business continuity plan requirements and priorities.

Conduct simple problem condition/scenario simulation of the single, compound, and cascading failures to define detailed plan content. Consider neighborhood environment potential impacts such as proximity to railways, refineries, airports, gas stations, etc.

Consider for each critical infrastructure component associated with each teleworking (home office) process whether an interruption would shut down the process, work function, or degrade performance. Would it prevent the key deliverable (e.g., customer bill) from being created and/or delivered? Also, how much time/effort is needed to recover the processing backlog of this remotely executed process? Who does this impact?

After identifying what risks need to be considered with the home office, each threat must be evaluated to determine the probability of it occurring and what impact it would have on workflow delivery within the organization. The likelihood of occurrence and effects can be assigned point values or a more general high, medium, or low rating.

À long terme, un plan de continuité des activités efficace peut aider une organisation à se démarquer de ses concurrents et à économiser beaucoup d'argent, de temps et de stress émotionnel.

La haute direction doit soutenir l'élaboration du plan de continuité des activités pour appuyer la politique de télétravail à l'échelle de l'entreprise. Les gestionnaires responsables du télétravail des employés devraient être directement impliqués dans la préparation du plan, car ils connaissent intimement les opérations et les fonctions de l'organisation et sont les plus susceptibles d'être au courant des faiblesses ou des vulnérabilités.

La première étape de l'élaboration d'un plan de continuité des activités consiste à définir et à inventorier les processus opérationnels qui seront exécutés ou sont actuellement exécutés à partir du bureau à domicile et à comprendre leur importance relative par rapport à d'autres fonctions et/ou activités de travail dans le cadre des supports de sortie (produits livrables). L'étape suivante consiste à déterminer la criticité de chaque processus métier et à déterminer lesquels doivent être préservés et rester opérationnels sans interruption, car ils sont essentiels aux opérations ou aux revenus de l'entreprise.

Une fois que la criticité des processus opérationnels est établie, y compris l'infrastructure requise, il faut déterminer les zones d'exposition au risque pour l'entreprise. Une évaluation des risques de haut niveau doit être réalisée pour identifier les points où les risques et les impacts sur la production et les revenus de l'entreprise sont les plus importants. Les scénarios de problèmes doivent être analysés afin de déterminer les exigences et les priorités du plan de continuité des activités.

Réaliser des simulations de problèmes simples et de scénarios de défaillances simples, composées et en cascade pour définir le contenu détaillé du plan. Tenir compte des impacts potentiels de l'environnement du voisinage, comme la proximité de chemins de fer, de raffineries, d'aéroports, de stations-service, etc.

Examinez pour chaque élément d'infrastructure critique associé à chaque processus de télétravail (bureau à domicile) si une interruption entraînerait l'arrêt du processus, de la fonction de travail ou la dégradation des performances. Cela empêcherait-il la création et/ou la livraison du produit clé (par exemple, la facture du client) ? En outre, combien de temps/efforts sont nécessaires pour récupérer le retard de traitement de ce processus exécuté à distance ? Qui est concerné ?

Après avoir identifié les risques à prendre en compte avec le bureau à domicile, chaque menace doit être évaluée pour déterminer la probabilité qu'elle se produise et l'impact qu'elle aurait sur l'exécution du travail au sein de l'organisation. La probabilité d'occurrence et les effets peuvent être attribués à des valeurs ponctuelles ou à une évaluation plus générale de niveau élevé, moyen ou faible.

Developing a business continuity plan for the teleworker is based on the various risks determined as of more significant concern for the 'home office location' to which the business process might be exposed, such as loss due to fire, flooding, severe weather, or loss of electrical power, natural gas, water supply, and heating or ventilation. Secondly, consider technology risks such as loss of telecommunication services (wireline, wireless, cable, and internet services) and computing technology failures (computer, data loss, applications (business systems), cable modem, and routers failures.)

In my experience, the risks that have the highest rate of occurrence in the home office are utility interruptions (power loss), technology failures (computers), and the loss of telecommunications (cell and/or internet access). The most straightforward business continuity plan (response and recovery) to any previous incidents is to ensure the individual has an alternate place of work to return to the central location of work (main office) to continue to deliver the workflow function. This assumes that a laptop has been issued (highly recommended) and all relevant business data and business systems, including collaboration tools remain operational at the alternate location.

The creation of a business continuity plan is not a one-time event. It must be regularly reviewed and updated to ensure that it reflects any changes to the facility, operations, or processes and lessons learned from incidents.

Training/awareness component via Exercising/testing the business continuity plan will reduce risk exposure and ensure the viability of the contingency solution and its implementation capability. An interruption can be compounded by the execution of an untested plan by unprepared personnel.

This guideline helps in identifying possible risks for teleworking (home-office) and provides suggestions, guidance, and best practices that could be introduced to minimize or eliminate these risks to your organization. Hoping for the best is not a plan!

You can't predict a disaster or emergency, but you can plan for one in advance. ■

**Vito Mangialardi, CBCP**  
is a Senior Business  
Continuity Management  
(BCM) Leader with  
more than 25 years of  
achievement delivering  
Business Continuity,  
Disaster Recovery Planning,  
Emergency, and Incident  
Management Programs in  
private and public sectors.



L'élaboration d'un plan de continuité des activités pour le télétravailleur est basée sur les différents risques déterminés comme étant les plus importants pour le "lieu de travail à domicile" auxquels le processus d'entreprise pourrait être exposé, tels que les pertes dues aux incendies, aux inondations, aux intempéries ou aux pannes d'électricité, de gaz naturel, d'eau, de chauffage ou de ventilation. Deuxièmement, considérez les risques technologiques tels que la perte de services de télécommunication (services filaires, sans fil, par câble et Internet) et les défaillances de la technologie informatique (ordinateurs, perte de données, applications (systèmes d'entreprise), modem câble et routeurs). )

D'après mon expérience, les risques qui ont le taux d'occurrence le plus élevé dans le bureau à domicile sont les interruptions des services publics (perte d'électricité), les défaillances technologiques (ordinateurs) et la perte des télécommunications (téléphone cellulaire et/ou accès à Internet). Le plan de continuité des activités le plus simple (réponse et récupération) en cas d'incidents antérieurs consiste à s'assurer que la personne dispose d'un autre lieu de travail pour retourner au lieu de travail central (bureau principal) afin de continuer à assurer la fonction de flux de travail. Cela suppose qu'un ordinateur portable ait été fourni (ce qui est fortement recommandé) et que toutes les données et tous les systèmes commerciaux pertinents, y compris les outils de collaboration, restent opérationnels sur le lieu de travail alternatif.

La création d'un plan de continuité des activités n'est pas un événement ponctuel. Il doit être régulièrement révisé et mis à jour pour s'assurer qu'il reflète les changements apportés aux installations, aux opérations ou aux processus, ainsi que les leçons tirées des incidents.

Composante formation/sensibilisation via L'exercice/test du plan de continuité des activités réduira l'exposition aux risques et garantira la viabilité de la solution d'urgence et sa capacité de mise en œuvre. Une interruption peut être aggravée par l'exécution d'un plan non testé par un personnel non préparé.

Ce guide aide à identifier les risques possibles du télétravail (bureau à domicile) et fournit des suggestions, des conseils et des meilleures pratiques qui pourraient être introduites pour minimiser ou éliminer ces risques pour votre organisation. Espérer le meilleur n'est pas un plan !

Vous ne pouvez pas prévoir une catastrophe ou une urgence, mais vous pouvez vous y préparer à l'avance. ■

**Vito Mangialardi, CBCP** est un responsable principal de la gestion de la continuité des activités (BCM), avec plus de 25 ans d'expérience dans la mise en œuvre de programmes de continuité des activités, de planification de la reprise après sinistre, de gestion des urgences et des incidents dans les secteurs privé et public.

What do I Do  
When I'm  
Not at Work?  
Volunteering and  
giving back to  
the community

Best Advice  
I Ever Got?  
Hire good people,  
teach them the  
skills to do  
the job.

Favourite  
Blogs...  
[newsinslowfrench.com](http://newsinslowfrench.com)  
[canada.ca/reconciliation](http://canada.ca/reconciliation)  
[canada.ca/lareconciliation](http://canada.ca/lareconciliation)

3 Goals  
for  
My Term...

3. Launch  
our next  
five year  
strategic plan.

Media:  
Instagram,  
Twitter,  
and I'm almost  
always taking an  
online course.

1. Submit my  
MBCP  
application!

2. Supporting  
veterans  
transition to  
BCM careers.

## Brock Holowachuk

CBCP, President DRIC,  
Chair of the Certification Commission

Manager, Reconciliation Communications  
Crown-Indigenous Relations and Northern  
Affairs Canada  
Government of Canada

Captain & Municipal Emergency Coordinator  
Springfield Fire and Rescue Service  
Rural Municipality of Springfield (Manitoba)

Que dois-je faire  
lorsque je ne suis  
pas au travail?

Faire du bénévolat  
et redonner à la  
communauté

Le meilleur conseil  
que j'ai jamais eu?

Embauchez de  
bonnes personnes,  
enseignez-leur les  
compétences pour  
faire le travail.

Blogs préférés...

[newsinslowfrench.com](http://newsinslowfrench.com)  
[canada.ca/reconciliation](http://canada.ca/reconciliation)  
[canada.ca/la-reconciliation](http://canada.ca/la-reconciliation)

3 Objectifs  
pour  
mon mandat:

3. Lancer  
notre  
prochain plan  
stratégique  
quinquennal.

Médias :  
Instagram, Twitter  
et moi suivons  
presque toujours  
un cours en ligne

1. Soumettre  
mon  
MBCP  
application!

2. Soutenir la  
transition  
des anciens  
combattants vers  
les carrières  
BCM.

## Advertisers' Index / Index des annonceurs

Sponsor	Page	Web site
Continuity & Resilience Today / J&J Expositions	2	<a href="http://crtdemcon.ca">crtdemcon.ca</a>
Benoit Racette Services-conseils inc.	7	<a href="http://racetteconseils.com">racetteconseils.com</a>
Mid-Range Computer Group Inc.	17	<a href="http://midrange.ca">midrange.ca</a>
Vanguard EMC Inc.	26	<a href="http://vanguardemergency.com">vanguardemergency.com</a>

erupting energy  
loss damaged  
eruption storm damage pollution  
tornado  
hurt  
environmental  
residential future dangerous survivor ruin  
natural disaster restoration warming  
city catastrophe flood  
communication survive tsunami rejuvenate destroy  
stormy world damage biological  
healthcare typhoon volcanic aid storm  
volunteers wind dirty  
natural hazard structure economy  
problem positive earthquake  
policy abandoned  
solution monitoring safety nature  
procedure illness economic old tremor  
attack recovery plan dam failure  
epidemic business continuity crater plan  
care danger continuity sabotage  
help climate resilience volcano charity  
crisis recovery planning  
weather management injured devastation  
incident natural preparation rescue team  
housing home disaster critical recession  
industry healing education fall-back  
fire environment destruction  
support survival infrastructure building insurance floods  
global tragic strategy explosion house  
broken hazard accident renovation protect vital  
victims hope prepare hurricane lost act  
panic improvement tragedy lives service  
debris risk protection violent  
chemical emergency  
severe warning  
upgrade magma  
threat human-induced  
cyclone continuation

