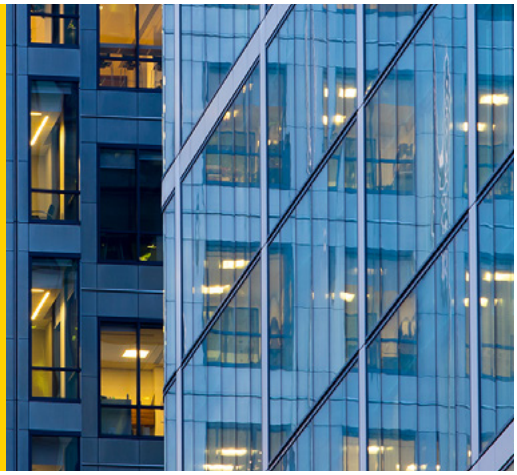


Preparing for the Unexpected: Business Continuity Trends and Tactics

AUGUST 2016

By Christopher Horne

Assistant Vice President, Information Technology Governance, Vendor Management, Security, and Business Continuity

For institutional investors, governments, regulators and stakeholders across financial services and other industry segments, there is increasing recognition of the role of business continuity in mitigating the effects of disruptive incidents on business operations and society. Organizations recognize the many cross-dependencies of today's inter-connected world – and seek assurance that their suppliers and partners have processes in place to mitigate the effects of unexpected incidents, disruptions and threats on critical services.

CIBC Mellon is trusted to safeguard more than C$1.6 trillion of assets on behalf of banks, pension plans, mutual funds, corporations and other institutional investors – a substantial portion of all the investable assets in Canada. We recognize the importance of our resilience to our clients, and we continuously work to further reinforce our strong governance and control environment. A key element of our company's commitment to clients is taking steps to plan, prepare and practice our responses to unexpected situations; we know we need to react to unplanned challenges in a prompt, organized and effective manner.

CIBC Mellon approaches business continuity holistically. CIBC Mellon's business continuity efforts are designed to provide our clients with confidence and assurance that risks related to the continuity of our business are appropriately assessed, monitored, managed and mitigated. Our approach includes clearly documented plans for each of our business units, multiple offsite recovery centres, and robust technology infrastructure via our parent companies, all combined with regular testing and exercises.

RECOGNIZING THE IMPORTANCE OF BUSINESS CONTINUITY MANAGEMENT

Business continuity management (BCM) is a holistic management process that identifies potential threats to an organization and the potential impacts to business operations of those threats, if realized; it is a framework for building organizational resilience capabilities, which can safeguard the interests of the organization's key stakeholders, reputation, brand and value-creating activities.

Business continuity should not be a one-time project, but rather should be constructed as an ongoing management and governance process supported by executive leadership and appropriately resourced. The process should identify potential impacts, maintain viable strategies and plans designed to mitigate those impacts, and should be kept vital and up to date with training, exercising, maintenance and review. Collaboration is also key: rather than containing effort within a single group, a business continuity process should engage business and operational leaders across an organization who are involved in the day-to-day delivery against organizational priorities.

CIBC MELLON

"As a leading Canadian custodian and asset servicing provider, we recognize the importance of our business to our clients. Our business continuity management efforts are designed to prepare our company and its employees to deliver essential services in unexpected circumstances."
– Christopher Horne, Assistant Vice President, Information Technology Governance, Vendor Management, Security, and Business Continuity, CIBC Mellon

"We are pleased to recognize and certify CIBC Mellon's achievement of the ISO 22301:2012 Societal Security and Business Continuity Management Systems Standard based on our comprehensive review and assessment of the systems, preparations, planning and response capabilities. CIBC Mellon's clients and stakeholders should take confidence from the diligence and effectiveness with which the company has undertaken business continuity planning." - Gary Robinson, Commercial Director, BSI Group Canada

Fundamentally, business continuity is a means to foster organizational resilience, preparation and vigilance. A carefully-considered, well-documented and actively-rehearsed business continuity regime allows an organization to provide confidence to its stakeholders that it is indeed operating within the parameters of the organization's risk appetite.

To that end, CIBC Mellon's business continuity team works collaboratively with management and representatives within every department and business unit at our company to develop, document, test and, when necessary, deploy business continuity plans to help CIBC Mellon respond to unexpected situations.

TRENDS IN BUSINESS CONTINUITY

The Business Continuity Institute (BCI) is a leading international membership and certifying organization for business continuity professionals worldwide. CIBC Mellon is an active participant in the organization, and CIBC Mellon's business continuity lead currently serves as President of BCI's Canada Chapter.

The Business Continuity Institute produces an annual Horizon Scan Report designed to track risks and threats to organizations through assessing perceived threats as shown by practitioners' in-house analysis. In the most recent Horizon Scan, the Business Continuity Institute tracked the following top trends according to 568 responding organizations in 74 countries:

Top 10 Business Continuity Threats: 2016 BCI Institute Horizon Scan

1. Cyber attack
2. Data breach
3. Unplanned IT & telecom outages
4. Act of terrorism
5. Security incident
6. Interruption to utility supply
7. Supply chain disruption
8. Adverse weather
9. Availability of talents / key skills
10. Health & safety incident

Technology matters remain at the forefront of industry focus, with a large majority of responding institutions identifying a cyber attack (85 per cent of respondents), data breach (80 per cent), and an unplanned IT outage (77 per cent) as areas about which they are "concerned" or "extremely concerned."

The specific impacts and risks related to these challenges, and the associated steps taken to mitigate related risks, vary substantially according to geography, industry, organization and many other factors. Adverse weather impacts in southeast Asia (monsoon flooding) may be markedly different from those in Canada (ice storm power outages), for example. Infrastructure vulnerability may also vary among jurisdictions, but regardless of strength, risks remain.

To illustrate, there is high confidence in Canada's utility supply infrastructure, but the 2003 blackout of eastern North America serves as a reminder that the unexpected can happen and has happened.

Sample Case: Executing BCP in response to July 2016 power outage in Toronto

On Wednesday, July 13, 2016, a brief power outage had an impact on a large area of the downtown core of Toronto, including CIBC Mellon's head office. The outage was attributed to high temperatures triggering high use of air conditioners, combined with a supply interruption in the infrastructure. While our office lost power momentarily, CIBC Mellon's business continuity preparations – which include emergency backup power systems – engaged as designed. CIBC Mellon responded to the incident according to its established business continuity management procedures. In view of the apparent triggers, and the likelihood that the weather pattern would persist, CIBC Mellon elected to engage a portion of its business continuity plan as a precaution. CIBC Mellon relocated more than 150 employees to alternate working locations over July 13 and 14. CIBC Mellon retained full operational capabilities throughout both days, and did not experience impacts to client deliverables as a result of the power outage or the execution of its business continuity plans. Throughout the response, additional coordination meetings and communications were completed throughout the day to monitor progress and completion of end of day business processing. Once a potential disruption was no longer a threat, our operations seamlessly returned to business as usual.

BUSINESS CONTINUITY INSTITUTE HORIZON SCAN 2016
Top Five Trends and Uncertainties and CIBC Mellon's responses

These five trends and uncertainties were cited by at least half of respondents to the BCI survey, and will likely find broad resonance among institutional investors.

1. Use of Internet for malicious attacks
2. Influence of social media
3. Loss of key employees
4. New regulations and increased regulatory scrutiny
5. Prevalence and high adoption of internet-dependent services

1. Use of Internet for malicious attacks

Cyber attacks and data breaches are key focus areas for many organizations responding to the BCI Horizon Scan survey, as practitioners remain particularly concerned about the potential for damage via cyber attacks and data breaches given the increased sophistication of hostile elements.

In an interconnected world, organizations of all sizes should place a high premium on IT governance, security and preparation. From internal processes to vendor management, organizations should seek to remain vigilant and work to continuously improve the controls and security measures in place to protect themselves and their stakeholders.

CIBC Mellon is well positioned with the support of two leading global financial services organizations – CIBC and BNY Mellon – both of which place a high premium on cyber security. CIBC, BNY Mellon and CIBC Mellon monitor the IT environment for potential threats and concerns, and work to further strengthen its security and governance measures.

CIBC Mellon and its parent companies have multiple levels of IT-related threat protection, and have implemented – and seek to continuously improve – a wide array of security measures designed to protect our company, clients, employees and the information under our control. We regularly receive security information on potential threats from our peers and the broader financial services industry, as well as our clients, law enforcement and a variety of public and private sources. CIBC Mellon and its parent companies monitor and assess our IT environments for potential vulnerabilities and threats, and continue to invest in and implement protections as deemed necessary.

At CIBC Mellon, we also work at the individual employee level – we work regularly with employees to raise awareness of the specific steps that they can take to help protect the company, its clients and the information under its control – from reporting phishing attempts to reinforcing controls around information handling, we know that employees' diligence and awareness of good practices is a critical element in our efforts to maintain strong controls.

2. Influence of social media

The growing influence of social media especially in relation to company reputation placed second in this year's report with 63 per cent of respondents concurring. In addition to concerns related to corporate reputation and the potential for brand damage, social media risks can include legal/regulatory compliance, security and privacy, and employee/HR issues[1].

Social media can also be a source of opportunity: social media monitoring can help an organization remain alert to potential threats and challenges and can provide a communication channel when an event happens. CIBC Mellon also uses social media to raise the profile of our great workplace experience, helping us recruit talented young professionals, so that we maintain a strong pipeline of talent to address natural turnover experienced at every organization.

Sample Case: The speed of social media

In 2010, Toronto played host to the global G20 summit in a location just blocks from CIBC Mellon's head office – an event expected to attract substantial protest activity to the downtown core. CIBC Mellon deployed its business continuity planning efforts well in advance, moving staff to alternate locations and preparing to deliver essential services. CIBC Mellon carefully monitored the social media environment throughout the event to remain alert for potential threats to the business or employees. When a tremor was felt through CIBC Mellon's 320 Bay Street head office during the event, social media conversation quickly identified the source of the tremor as a minor 5.0 earthquake impacting Southern Ontario, in turn helping forestall employee concern and maintain focus on the work at hand.

3. Loss of key employees

Every business depends on key players to deliver strong results. The "human factor" (i.e. skills shortage, loss of key employees) is a major focus area for business continuity management as a field. An organization's planning, documentation and response to an issue will significantly depend on the ability of its teams to react quickly and effectively.

From a business continuity perspective, we recognize the critical role that employees play. Every business unit at CIBC Mellon has a designated Business Recovery Planning Coordinator and Alternate who collaborate with the company's business continuity team to assess and document the business unit's business continuity needs and plans. Our plans encompass a wide array of factors, such as identifying business functions as time-sensitive and critical (for example, transaction processing) or more general business activities that can take a lower priority during a business continuity issue (for example, tax research). From working remotely to shifting to alternate offsite recovery locations to the specific technical and connectivity requirements of each employee's role and tasks, we work to document the needs of our teams, which in turn positions us to plan for, maintain and deploy critical capabilities during an incident.

An effective HR recruitment and retention strategy can also help mitigate risks related to loss of key employees. "Engaging Employees" is a key focus area for CIBC Mellon as we work to attract, retain and motivate talented individuals, and deliver robust programming to support employee engagement: CIBC Mellon was once again named one of the Achievers 50 Most Engaged Workplaces in North America in 2016. In 2015, the company also earned a Canadian HR Award for "best reward and recognition strategy," and was highly commended for its volunteering program in the "CSR Project of the Year" category at the 2015 Employee Engagement Awards. At CIBC Mellon, we recognize the critical importance of investing in a workforce that is committed to doing well by doing right, and engaged in delivering services for clients. Employees focused on delivery will deliver on continuity plans as well.

4. New regulations and increased regulatory scrutiny

Today's financial services market participants direct substantial attention to compliance with requirements from various industry and regulatory bodies in Canada. From the Office of the Superintendent of Financial Institutions (OSFI)'s outsourcing guidelines to the Financial Services Commission of Ontario (FSCO)'s records retention needs, regulatory expectations demand that suppliers are able to provide confidence to their customers that risks related to business continuity are being well-managed. With this in mind, CIBC Mellon provides its clients with detailed reporting on controls, practices and governance efforts, and makes available an overview of the steps CIBC Mellon takes with regard to business continuity efforts.

Supporting resources from a regulatory and industry perspective are available to help organizations be aware of threats and trends, and to help them prepare to respond. Examples of some programs and articles published by North American authoritative entities include:

- Business Continuity Institute annual Horizon Scan Report
- The Business Continuity Institute – The Good Practice Guidelines (GPG)
- ISO 22301 Societal Security and Business Continuity Management Systems Standard
- Federal Financial Institutions Examination Council Handbook on Business Continuity Planning
- Canadian Standards Association Z1600 Emergency Management and Business Continuity Programs
- National Fire Prevention Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs

Are you prepared?

Preparing properly for an emergency should include documented plans to support employees and the business in responding to a wide array of emergency or issues management situations. To fully prepare, CIBC Mellon has specific procedures in place to execute at each stage of an emergency:

Emergency Response: Actions to be taken that minimize or contain negative effects, preserve lives, and provide basic services following the immediate aftermath of a disaster. These actions should continue for as long as an emergency situation prevails.

Incident Management: A plan of action for use at the time of an incident that encompasses key personnel, resources, services and actions needed to implement the corporate incident management process and initiate recovery procedures.

Business Recovery: Steps required to support the continuation or resumption of business activities within an acceptable timeframe during or following a disruption.

Disaster Recovery/Service Continuity: Planning required to recover and restore technological infrastructure and capabilities after a serious interruption, including activities to restore necessary IT infrastructure required to support critical business functions.

5. Prevalence and high adoption of internet-dependent services

For organizations across the spectrum, the internet is a critical connection between systems, people and organizations. From cloud services to email communications, organizations must carefully consider how to assure themselves and their stakeholders that appropriate steps have been taken regarding the use of internet-enabled services. To respond to risks related to internet-enabled services, organizations must appropriately review service providers – not only before and during vendor selection and onboarding, but also as an ongoing process. Effective business continuity includes putting controls and standards in place to help provide assurance that vendors continue to maintain alignment to agreed-upon standards as well as to emerging needs and threats. Vendors may provide assurance across many factors, such as multiple redundant/backup data centres, detailed disaster recovery/service continuity planning, and high standards for information security.

CIBC Mellon leverages powerful and robust infrastructure from CIBC and BNY Mellon, together with extensive vendor management processes to support confidence around internet-enabled services. We work to carefully assess vendors to confirm their alignment to our standards, and we leverage the expertise and scale of our two parent companies to help us monitor the IT environment. We provide all employees with detailed annual training related to information security, and work to monitor for emerging threats on an ongoing basis.

GUIDING PRINCIPLES FOR A BUSINESS CONTINUITY PROGRAM

Service reliability and systems resilience are critical components of modern business continuity management, with a key focus on continuity of communications and business operations via recovery processes executed in conjunction with key suppliers and stakeholders.

CIBC Mellon promotes and facilitates business continuity through a detailed and centrally coordinated business continuity program, which is updated and tested to respond to market and industry changes. Our plan focuses on leveraging multiple geographies available to us via our parent companies, use of multiple back-up facilities, and resources dedicated to the business continuity process. We have designed our program to allow critical operations to continue in a broad range of circumstances, including significant regional power outages and natural or human-made disasters. CIBC Mellon's business continuity plans are coordinated with its parent companies CIBC and BNY Mellon, and CIBC Mellon maintains multiple geographic locations to mitigate risks.

CIBC Mellon has built its business continuity program around a set of guiding principles:

- Enterprise-wide business continuity governance residing with a senior executive
- Planning and testing procedures across all businesses and critical technologies
- Geographic diversification of critical operations and technology processing centres
- Utilization of remote, timely data replication designed for rapid systems recovery and protection from data loss
- Back-up telecommunication circuits that are diversified from primary circuits
- Back-up systems that meet or exceed processing and regulatory requirements

LIFE CYCLE PLANNING

We live in an ever-changing world, and every business has regular turnover across employees, locations, technology and suppliers. To help maximize effectiveness, business continuity planning must be a repeatable process that continuously considers change management and new initiatives, and projects holistically from inception through implementation. At minimum, requirements should be reviewed annually, but changes need to be operationalized in planning before or as near to when they occur.

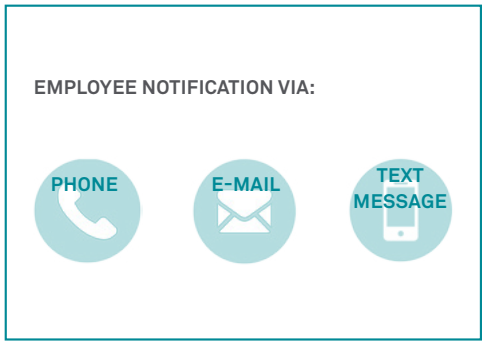
Cellphone Essentials: every employee should keep these numbers in their mobile phone:

- A speed dial number for the organization's central alert line or a set conference bridge number for use in emergencies
- Their manager's work, home and cellphone numbers
- Any direct reports' work, home and cellphone numbers
- Other emergency numbers, including their Business Unit's conference bridge number (if applicable)

ENTERPRISE CRITICAL COMMUNICATIONS

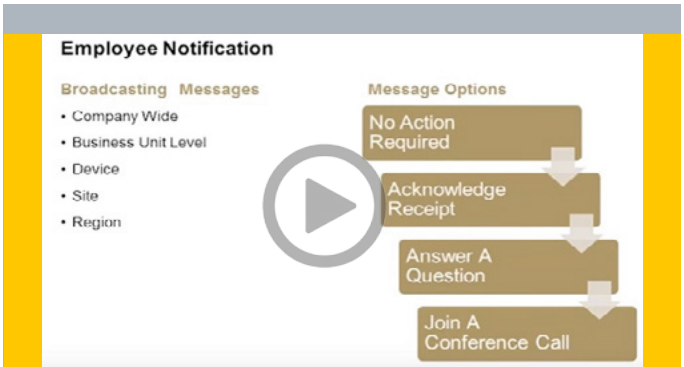
A critical factor in supporting an organization's effective response is its ability to communicate – not only with its external suppliers and clients, but within the organization itself. Effective planning will count for little if the necessary employees are not advised to enact those plans in a prompt manner. Communication challenges can be further compounded during an incident – for example, employees are often away from their business email systems outside business hours. Sometimes an incident itself – such as a power outage – may directly impact the ability of employees to access communications via traditional channels. Speed is also a concern: call-tree structures that depend on managers calling their teams and providing up-to-date information can be compounded by multiple levels of management. Call trees are also subject to service availability risk, as during large scale regional incidents, cell networks can be overwhelmed and limited to text messages or potentially become unavailable.

CIBC Mellon has implemented an enterprise critical communication system provided by Everbridge. This system helps CIBC Mellon rapidly deploy two-way mass communication with employees across multiple channels, including email, business and personal phones, text messages and more. Within minutes, CIBC Mellon can provide updates to apprise employees of an issue, provide guidance (for example, to work from an alternate location), or even capture survey responses to confirm employee safety, availability and weather impacts at their locations. The system is connected with a secure daily feed from the company's human resources information system, keeping information up-to-date.



Short overview of CIBC Mellon leveraging the Everbridge Critical Communication System

For a detailed overview of CIBC Mellon's enterprise critical communication capabilities and strategies, view the linked one-hour overview webinar featuring Christopher Horne, Assistant Vice President, Information Technology Governance, Vendor Management, Security, and Business Continuity, CIBC Mellon. Recorded in 2015, the webinar provides participants with insights on how CIBC Mellon leverages the Everbridge enterprise critical communications system to position the company to rapidly engage employees in business continuity response – for example, monitoring current local emergency events (e.g. fire, flood), confirming whether employees are able to reach the office during a major snowstorm, or directing employees to alternate working locations in the event that a primary office is unavailable.



https://youtu.be/u8w4BO9_5do

ISO 22301:2012 is a management systems standard for BCM which can be used by organizations of all sizes and types. These organizations will be able to obtain accredited certification against this standard and demonstrate to legislators, regulators, customers, prospective customers and other interested parties that they are adhering to good practice in BCM. ISO 22301:2012 also enables the business continuity manager to show top management that a recognized standard has been achieved.

Download the Everbridge paper featuring CIBC Mellon as a case study highlighting good practices for proactive threat monitoring and critical response.

THIRD PARTY ASSURANCE AND CERTIFICATION

Prior to the turn of the millennium, continuity and contingency planning and disaster recovery were largely information technology-led responses to natural disasters and terrorism. Organizations focused on fire safety, emergency power supplies, and call-tree notification of staff. Preparations were largely focused on physical and technology processes, with business process and services viewed as a secondary concern. Today, there has been a move from "crisis management" to "business continuity", with a focus not only on safeguarding life and facilities, but also on maintaining continuity of critical services for an organization's stakeholders.

As governments, regulators, customers and other stakeholders seek assurance that key suppliers and partners are in position to provide key products and services, even when incidents occur, demand has grown for tools and frameworks to assist organizations in interacting with their suppliers, counterparties and customers, specifically related to providing confidence through business continuity management. In response to significant global interest, cooperation and input, the International Standards Association developed ISO 22301:2012, Societal security – Business continuity management systems – Requirements.

CIBC Mellon has aligned its Business Continuity Management program to the International Organization for Standardization (ISO) standard for Business Continuity Management (BCM) Systems, specifically ISO 22301:2012, and has been granted certification to the standard. ISO 22301:2012 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of, prepare for, respond to, and recover from disruptive incidents when they arise.

To achieve ISO 22301:2012 certification, CIBC Mellon's business continuity preparations were assessed by external auditors from the British Standards Institution (BSI Group) Canada. CIBC Mellon's business continuity plans are highly flexible, enabling it to respond to different scenarios, and the company can execute all or a portion of its plans depending on the type, severity and impacts of an event. Response planning encompasses preparations for CIBC Mellon's employees, offices, technology and supply chain, with the aims of preserving life safety, quickly organizing CIBC Mellon's response to an incident, maintaining service continuity, and rapidly recovering any impacted services to clients. The ISO 22301:2012 certification applies to the Canadian operations of CIBC Mellon Global Securities Services Company and CIBC Mellon Trust Company.

REGULAR TESTING AND EXERCISES

Business continuity plans are critically dependent on the ability of staff to develop, document and most importantly, execute plans effectively. In addition to traditional planning such as how to respond to a building fire alarm, employees must be familiar with the business expectations placed on them during an incident (for example, whether they should head to a secondary office, work remotely, or simply await the business' return to regular operations). Employees should also be familiar with the communications tools and the means by which they will be advised. Likewise, senior managers involved in leading the company's response should have familiarity with the available tools and their decision-making responsibilities during an incident, helping to validate strategies as well as support enhanced response times. When employees know where to go and what to do, an organization can respond more effectively to an unexpected incident.

At CIBC Mellon, we engage in regular exercises of our plans in order to train employees as well as to validate our strategies, documentation and technology. CIBC Mellon conducts regular after-hours communication exercises to all employees, as well as exercises that see employees enact alternate working plans for a regular business day.

CIBC Mellon's Incident Management Plan (Crisis Management Plan) is exercised in an annual business continuity "table-top" exercise. This event sees our Incident Management Team, whose membership includes the Executive Committee and senior leaders from every business unit at CIBC Mellon, respond in real time to a simulated emergency, complete with unexpected developments throughout. In addition to valuable practice, the exercise provides an opportunity for the team to come together for a post-event assessment in order to seek opportunities for further enhancement.

PREPARING FOR THE UNEXPECTED: BUSINESS CONTINUITY PLANNING CONSIDERATIONS

While many aspects of planning for incidents might be considered "common sense" (for example, clearly signing fire exits and running employee evacuation drills), modern business continuity practice is about working to put steps in place that position an organization to meet its commitments even during challenging, unexpected or highly disruptive circumstances, and to enable a capability to respond flexibly to a wide array of possible scenarios.

Business continuity is about building and improving organizational resilience, including clearly assessing the risks, expectations and dependencies attached to key products and services. An organization should work to investigate, understand and document the activities, systems and people that help underpin critical organizational commitments. With effectively devised business continuity plans and strategies, an organization can position itself to carry out its operations and business operations during and following an incident, crisis or disaster, and to recover quickly and effectively from any type of disruption. While no business or organization can absolutely guarantee against any and all potential disruptions, a strong plan, engaged employees and robust systems can help provide stability, mitigate risk and enable an organization to best serve its stakeholders during the most challenging times.

Learn More

To learn more about CIBC Mellon's approach to business continuity, contact your Relationship Executive or Service Director, or visit www.cibcmellon.com/businesscontinuity.

Business Continuity Questions to Consider

- Does your organization have an active and ongoing business continuity process?
- What critical business or service commitments has your organization made to its clients and stakeholders?
- How does your organization document its business continuity plans and needs?
- How does your organization plan to communicate to its employees, clients and other stakeholders during an emergency or crisis? How would you reach people outside regular business hours?
- What are your organization's critical dependencies, technologies and systems?
- Who are your essential employees?
- Who are your critical vendors, and how have you worked to satisfy yourself and your own stakeholders that those vendors are prepared for a disruption?
- What regulatory, Board or stakeholder reporting requirements call for your organization to address business continuity preparations?

Notes:

1 https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-managing-social-media-risks-reputation-risk-03032015.pdf

CIBC MELLON

A BNY MELLON AND CIBC JOINT VENTURE COMPANY℠

000 - KL24 - 08 - 16