Abstract
As the pace of change in information technology (IT) accelerates, business continuity management (BCM) continues to evolve rapidly within enterprises to meet increased market and regulatory demands. Significant business and technology changes need to be assessed by the enterprise from many perspectives, including impact on existing processes, associated risk and how technology changes can be leveraged to improve continuity capabilities. This white paper provides an overview of the impacts, benefits and opportunities of four emerging technologies (virtualization, cloud computing, mobile devices and social networks) as they relate to BCM.
About ISACA®
With more than 100,000 constituents in 180 countries, ISACA (www.isaca.org) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the ISACA® Journal, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA continually updates and expands the practical guidance and product family based on the COBIT® framework. COBIT helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer
ISACA has designed and created Business Continuity Management: Emerging Trends (the “Work”) primarily as an educational resource for governance and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, governance and assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights
© 2012 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide feedback: www.isaca.org/Business-Continuity
Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center
Follow ISACA on Twitter: https://twitter.com/ISACA
Join ISACA on LinkedIn: ISACA (Official), http://linkd.in/ISACAOfficial
Like ISACA on Facebook: www.facebook.com/ISACAHQ

Business Continuity Management: Emerging Trends
Acknowledgments

ISACA wishes to recognize:

Project Development Team
Salomon Rico, CISA, CISM, CGEIT, Deloitte LLP, Mexico, Chair
Daniel Dec, CISA, CISM, Cognizant Technology Solutions, USA
Scott Shinners, CISA, CPA, ConAgra Foods Inc., USA

Expert Reviewers
Richard B. Fowler, CISA, CFE, CIA, CICA, Huntington Ingalls Industries, USA
Ayman M. Galal, CISA, CISM, CGEIT, CRISC, CISSP, Accenture, UK
Inigo Garcia Merino, CISA, Deloitte S.L., Spain
Elliott C. Jolesch, USA
Norbert Kuiper, CISA, CISM, Centric IT Solutions, The Netherlands
Andre Quint, CISM, AMBCI, ASR Nederland, The Netherlands
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium
Erika Voss, CORM, CGI Federal, USA
Terry L. Whaley, CISA, CGEIT, CRISC, CIA, USA

ISACA Board of Directors
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, International President
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Vice President
Juan Luis Carselle, CISA, CGEIT, CRISC, Wal-Mart, Mexico, Vice President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Ramses Gallego, CISA, CGEIT, CSEK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIQA, Queensland Government, Australia, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., USA, Vice President
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Past International President
Emil D’Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., (retired), USA, Past International President
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapore, Director
Kristen McCabe, CISA, The Home Depot, USA, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Australia, Director

Knowledge Board
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Thomas E. Borton, CISA, CISM, CRISC, CISSP, Cost Plus, USA
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Salomon Rico, CISA, CISM, CGEIT, Deloitte LLP, Mexico

Guidance and Practices Committee
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
Dan Haley, CISA, CGEIT, CRISC, MCP, Johnson & Johnson, USA
Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France
Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Vista Point, Brazil
Jotham Nyamari, CISA, Deloitte, USA
Connie Lynn Spinelli, CISA, CRISC, CFE, CGMA, CIA, CISSP, CMA, CPA, GRC Solutions LLC, USA
John William Walker, CISM, CRISC, FBCS CITP, ITPC Secure Bastion Ltd., UK
Siang Jun Julia Yeo, CPA (Australia), Visa Worldwide Pte. Limited, Singapore
Nikolaos Zacharopoulos, CISA, CISSP, DeutschePost–DHL, Germany
Acknowledgments (cont.)

ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors
Information Security Forum
Institute of Management Accountants Inc.
ISACA chapters
ITGI France
ITGI Japan
Norwich University
Socitum Performance Management Group
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School

ASIS International
Hewlett-Packard
IBM
Symantec Corp.
Introduction

Recent events and natural disasters resulting in business disruptions around the world illustrate the importance of having a robust and mature business continuity management (BCM) program as part of the enterprise strategic planning process. BCM moves to the forefront each time the news reports a major catastrophe, which demonstrates the value of building resilient infrastructures, designing sustainable supply chains and defining communication and contingency procedures to restore critical business operations within acceptable recovery times.

BCM is an established component of risk management in many enterprises, and a common practice within BCM is to conduct business impact analysis (BIA) periodically or every time a significant change occurs within the enterprise. Many changes are anticipated and planned (e.g., moving data centers, implementing new systems, migrating process to third-party providers, virtualizing systems, adopting cloud computing) while other changes, such as fundamental shifts in processes, business practices or supporting technologies (e.g., new market demands, new legislation or regulation, using social networks and mobile devices for business purposes) may not be anticipated or planned. All of these changes require the different parties involved in BCM to assess the scope and nature of issues that may arise, and work with business owners to identify necessary changes to existing continuity and recovery plans to reflect the new environment. It is important to note that some changes, especially in technology, can represent opportunities to improve BCM automation and recovery times and optimize the cost associated with continuity activities.

Continuity needs are unique to each enterprise; however, there are common considerations that should be followed when planning an initial BCM program or modifying an existing one to address changes within the enterprise and the external environment. This white paper provides an overview of the potential impacts that emerging technology trends can have on BCM. It identifies potential benefits, challenges, governance and risk management practices, and provides an overview of relevant assurance considerations related to continuity management.

Terminology

BCM is a set of processes and resources to identify possible threats, calculate their potential impact and provide the necessary practices to prevent, mitigate and recover from disruptions. The most common BCM processes include disaster recovery, crisis management, incident response management and contingency planning.

Business continuity (BC) and disaster recovery (DR) are sometimes used interchangeably; however, their focus and scope are different. BC is a broader term that encompasses developing, testing, and managing enterprisewide continuity plans while DR is the process focused on building continuity capabilities for critical IT infrastructure and business applications. Some enterprises use the term BC/DR to note the close relationship.

In addition to DR, the key components of BCM are:

- Crisis management (CM)—Defines the steps necessary to address and mitigate the effect of a negative event, often while the event is still happening (e.g., fire, tornado, earthquake, severe weather)
- Incident response management (IRM)—Defines the necessary steps to address and minimize the negative impact of a physical or logical incident threatening enterprise resources (people, physical and logical assets), e.g., theft, security breach or natural disasters
- Contingency planning—Process of developing advance arrangements and procedures that enable an enterprise to respond to an event that could occur by chance or unforeseen circumstances
• **Business impact analysis (BIA)**—Is a process to determine the impact of losing the support of any resource (people, facilities, systems, information, etc.) and define the order in which resources should be restored based on their criticality to the business. Two important elements for the plan are calculated using BIA information:
  – **Recovery time objective (RTO)**—Defines the time allowed for the recovery of a business function or supporting resources after a disruption/disaster occurs
  – **Recovery point objective (RPO)**—Quantifies the permissible amount of data loss in case of interruption and defines the earliest point in time that is acceptable to recover data

### Business Trend and Emerging Technology Impact on BCM

The business environment is changing rapidly as enterprises of all sizes move to real-time operations around the world on a 24/7 basis. Connectivity and real-time information have become increasingly important for the successful operation of global strategies for most enterprises and are expected by clients, employees and business partners as part of normal operations. Some of the trends impacting the business landscape include globalization, electronic commerce, single-instance enterprise resource planning (ERP) systems, increased and expanding regulation and mobile computing in the workplace. Therefore, faster ubiquitous connectivity, real-time information and 24/7 availability have become critical to retaining competitive advantage for a large number of enterprises. Advanced technologies are the primary enablers for the way the world conducts business and, by consequence, a critical part of BCM. Emerging technologies (virtualization, cloud computing, mobile devices, social networks) are already impacting enterprises by introducing new challenges, risk and opportunities that must be either addressed or exploited.

### Rapidly Changing Business Environment

The rapid pace of business and technology changes coupled with increasing performance expectations from customers, employees and management apply constant pressure on IT infrastructures and supporting teams to provide around-the-clock availability and minimize planned and unplanned disruptions. To adapt and respond to such demands under both normal and adverse conditions the enterprise should incorporate robust technology adoption policies and procedures and recovery solutions that are tested periodically as part of the BCM program.

### Global Operations

The shift of IT services to specialized third-party service providers is driving higher expectations of greater utilization and efficiency. While there are both financial and performance improvements associated with a greater resource and infrastructure mix (internal IT, outsourcing and offshoring), there are also new threats and vulnerabilities to business performance, security and continuity arising from growing interdependencies with third-party service providers. These interdependencies make it all the more critical to anticipate and plan how to respond in the event of a disruption or natural disaster affecting a third-party service provider.

### Regulatory Scrutiny

The disperse storage or processing of data exposes enterprises to potential legal and regulatory risk. In some cases there may be no legal precedent to define roles, responsibilities and liabilities of data owners and service providers across jurisdictions. Therefore, it is vital that enterprises secure, under contract, the right to know the ultimate location of its data and defines clear roles, responsibilities and liabilities relative to legal and regulatory requirements.
Emerging Technologies
To face the challenges posed by new business and regulatory trends, enterprises need to adopt technologies that enable high-availability systems, real-time communications and faster recovery times while minimizing IT cost. Advances in telecommunications, more user-friendly technology, improved data storage solutions, cost-effective virtualized environments, and cloud computing are enabling enterprises to increase data storage capabilities, become agile and improve business resilience. Other trends, such as mobile devices and social networks, are improving the way enterprises communicate, interact and collaborate with customers, suppliers, employees, government agencies and peers during a business disruption.

Emerging Technology Benefits for BCM
Financial and strategic objectives can be achieved through effective utilization of emerging technologies within a BCM program. However, to realize these objectives the enterprise needs to first address new risk introduced through the adoption of new technologies to minimize negative impacts and maximize benefits. Managing risk effectively enables senior management to make better decisions for aligning BCM with business and IT strategies to eliminate redundancies, manage resources efficiently and still meet shareholder, customer and regulatory expectations and requirements for resilience and recovery capabilities.

Recovery Time and Data Loss
Advances in data storage and replication technologies (e.g., data vaulting, backup to disk, deduplication), and advances in telecommunications enabling high-speed bandwidth at lower cost have enabled some enterprises to increase data storage and replication capabilities. These enterprises have implemented solutions to electronically replicate and synchronize data and programs offsite more often to improve the resilience of critical business functions and enable a reduction in the time it takes to gain access to backup data in case of a disaster. Better data storage capabilities make it possible to meet optimal RPOs after a business disruption.

In addition to better backup technologies, server virtualization can help decrease the time needed to restore critical applications to full functionality. Disaster recovery plans that take advantage of virtualization require less physical resources and administrative personnel to restore critical applications within the established RTOs.

Mobile devices in the workforce allow for faster work force recovery. The ability to access enterprise resources using laptops, tablets and smart phones represents a significant advantage for employees who cannot travel to the physical location of the enterprise, and for the enterprise because employees can remain productive during disruptive events without the need to provide temporary work space and computing resources.

Improved Resilience
Server virtualization and cloud computing help reduce planned outages by providing the ability to move applications to temporary environments during system maintenance, firmware upgrades, critical patching and DR testing. Unplanned outages can also be minimized due to the ability to take configuration snapshots of mission-critical virtual machines and restore them using similar hardware devices in shorter periods of time within the same data center or across geographic areas.
Virtual desktop infrastructure (VDI) has a positive impact on BCM because it enables more distributed work forces and access to critical applications during a disaster. As long as employees can access the Internet, they will have access to applications configured to be delivered using virtual desktops; this can minimize productivity loss and reputational damage resulting from poor customer support during an outage. Leveraging VDI as part of the BCM strategy can help reduce the cost associated with work area recovery because the efforts to recover physical facilities may be spread over longer periods of time without sacrificing productivity or efficiency.

Some of the cloud computing services having the greatest impact on BCM are: Disaster Recovery or Replication as a Service (DRaaS), Backup as a Service (BaaS), Storage as a Service (STaaS) and Software as a Service (SaaS). The main advantage of these services is that they can help enterprises improve resiliency while maintaining the initial investment cost and keeping down the operating cost. DRaaS is a cost-effective alternative to maintaining a second location for DR purposes; this solution can follow the “pay per use” model or require minimal fees to retain services that combine networking, computing and storage infrastructure on stand-by. SaaS improves resilience by allowing employees to access applications remotely via the Internet. Ensuring continuity for cloud services is the responsibility of the cloud service provider; however, the enterprise must be diligent during contract negotiations and establish service level agreements (SLAs) that clearly define continuity expectations for critical applications and, if necessary, maintain internal contingency plans to alleviate vendor failure to meet SLAs.

**Cost Efficiency**

One of the most evident benefits of adopting cloud computing services is the minimal investment required to turn services on and the lower operating cost associated with managing cloud services. Virtualization and virtualized server management tools enable enterprises to reduce the number of IT assets and administrative personnel needed to provide system redundancy and reduce system recovery time. Furthermore, virtualization and cloud computing services can be used to test DR and BC plans and save money by turning off services after testing is complete (pay per use). One of the most evident benefits of adopting cloud computing services is the minimal investment required to turn services on and the lower operating cost associated with managing cloud services.

Mobile devices in the workforce can also help enterprises minimize cost associated with BC because mobile devices may be a cheaper option than providing traditional computer equipment for home use or for temporary use during the disruption. Another cost reduction can be realized by eliminating the need for temporary work space because employees can work from any location.

Rather than placing costly ads in newspapers and keeping expensive telecommunications subscriptions, enterprises can use social networks to provide the same information to larger audiences around the world at a speed closer to real time.

**Communications**

Automated notification systems have replaced manual call-tree processes. These automated systems can be linked to human resource (HR) databases to update employee information efficiently and in a timely manner, thus reducing the risk of using outdated contact information during a critical time. Messages can be distributed using voice, short message service (SMS) or email and received using mobile devices.

Storing business continuity plans (BCPs) and disaster recovery plans (DRPs) off site has been part of best practices for a long time, but now with the proliferation of mobile devices making plans accessible via these devices is also becoming an area of focus for parties involved in the different areas of BCM. Efficiency can be improved if employees can begin recovery tasks soon after the disaster is declared instead of having to wait until the plans can be retrieved from the offsite location.
Proper communication with employees and suppliers also can improve efficiency. Mobile devices allow continuity coordinators to contact key personnel and direct them where to go, what to do, or simply provide status updates to keep uncertainty and panic to a minimum.

Social networks can be an efficient way to communicate during a disaster. Enterprises can use these media to provide updates to customers and employees, and collaborate with other enterprises and suppliers dealing with similar problems. A word of caution for enterprises using social networks is to always craft messages that protect their integrity and reputation and avoid placing sensitive information on social media. This can be accomplished by appointing and training people qualified to communicate effectively over many communication channels, including social media, during and after a crisis. Proper planning to determine whether social networks should be part of BCM can help reduce the risk of doing more harm than good during a crisis.

**BCM Strategies**

*Figure 1* provides a list of BCM strategy considerations related to business trends and emerging technologies.

<table>
<thead>
<tr>
<th>Area of Consideration</th>
<th>Impacts</th>
<th>BCM Strategy Considerations</th>
</tr>
</thead>
</table>
| **Globalization**     | • Increased complexity and variety of BCM constituencies  
                        • Increased number and variety of potential recovery facilities, including hosting, shared and mobile sites  
                        • Increased number of vulnerabilities and threats  
                        • Greater likelihood and impact of business interruption  
                        • Increased complexity in supply chain channels  
                        • Increased number of stakeholders who require BCM training and awareness | • The enterprise should develop and communicate consistent policies and procedures guiding BCM across all geographic areas.  
 • BCM should be communicated to and coordinated with ERM to ensure alignment and eliminate duplication of efforts.  
 • BCM plans should be updated to reflect any significant change to business processes, organizational structures and IT infrastructures.  
 • Backups must be tested periodically to validate that data can be restored within the established RPO and RTO.  
 • BCM should leverage dispersed geographic locations to implement redundant systems and/or distributed processing.  
 • BCM should leverage the availability of cost-effective technologies that allow data duplication and synchronization across logical and physical environments located in dispersed locations.  
 • BCM training and awareness should be conducted periodically.  
 • Each physical location should maintain BCPs that align with enterprise BCM.  
 • The enterprise should require critical vendors/ suppliers to implement and maintain continuity plans that align with the enterprise’s continuity plan. |
| **E-commerce**        | • Increased demand for real-time transactions  
                        • Increased demand for uptime/high availability of business processes supporting e-commerce  
                        • Increased reliance on technology to complete business transactions  
                        • Elimination of clear geographic boundaries | • BIA for critical functions must be updated frequently to ensure that continuity plans are adequate.  
 • BCM testing should be conducted frequently to ensure that continuity capabilities are adequate.  
 • Data classification must be part of BCM to identify all critical data supporting e-commerce.  
 • Advance backup technologies (online replication) should be considered as part of BCM strategies dealing with critical data.  
 • Backups must be tested periodically to validate that data can be restored within the established RPO and RTO.  
 • BCM should consider using virtual environments to implement cost-efficient redundancy. |
<table>
<thead>
<tr>
<th>Area of Consideration</th>
<th>Impacts</th>
<th>BCM Strategy Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market pressure</td>
<td>• Increased demand for high availability systems</td>
<td>• BCM testing and validation must be conducted periodically to ensure that plans are relevant and effective.</td>
</tr>
<tr>
<td></td>
<td>• Increased competition within industries</td>
<td>• BCM capabilities should be developed with the intention of creating competitive advantage.</td>
</tr>
<tr>
<td></td>
<td>• Increased single-point-of-failure due to consolidation of vendors/suppliers</td>
<td>• IT hosting service providers must conduct periodic dry run testing to demonstrate their ability to meet continuity requirements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Contracts and SLAs should include specific clauses addressing continuity requirements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enterprises should maintain contingency plans to address critical-vendor failures.</td>
</tr>
<tr>
<td>Regulatory/legal requirements</td>
<td>• Increased awareness by senior management due to expanding regulatory requirements</td>
<td>• BCM should be aligned with business and IT strategies to ensure that regulatory and legal requirements are met.</td>
</tr>
<tr>
<td></td>
<td>• Increased privacy legislation</td>
<td>• BCM policies and procedures should incorporate the necessary controls to ensure that data integrity and privacy are not compromised during recovery efforts.</td>
</tr>
<tr>
<td></td>
<td>• Increased reporting requirements based on risk</td>
<td>• BCM consideration should be included in system development life cycle (SDLC) and change management policies and procedures.</td>
</tr>
<tr>
<td>Server virtualization</td>
<td>• Decreased number of physical assets needed to support IT infrastructure</td>
<td>• An inventory of virtual systems must be maintained to ensure that critical systems are included in BC/DR plans.</td>
</tr>
<tr>
<td></td>
<td>• Decreased number of administrative personnel needed to support virtual environments</td>
<td>• Virtual assets must be part of asset classification efforts to ensure that critical systems are identified and included in BC/DR.</td>
</tr>
<tr>
<td></td>
<td>• More centralized server management</td>
<td>• Virtual systems must be hardened to increase resilience.</td>
</tr>
<tr>
<td></td>
<td>• Increased redundancy capability</td>
<td>• Virtual servers should be considered as options to provide greater recovery capabilities at lower cost.</td>
</tr>
<tr>
<td></td>
<td>• Reduced maintenance downtime</td>
<td>• Virtual disaster recovery environments must be tested periodically.</td>
</tr>
<tr>
<td></td>
<td>• Decreased dependency on homogeneous physical assets</td>
<td>• VDI can be a cost-effective alternative to securing temporary work space during a disaster.</td>
</tr>
<tr>
<td>Desktop virtualization</td>
<td>• Expansion of the work space to remote locations</td>
<td>• Critical business functions should consider using desktop virtualization to increase continuity and productivity during a crisis.</td>
</tr>
<tr>
<td></td>
<td>• Faster desktop deployment</td>
<td>• Virtual desktops delivered over the Internet must be protected using secure tunneling.</td>
</tr>
<tr>
<td></td>
<td>• Centralized desktop management</td>
<td>• In-house backups for critical data must be continued to ensure recovery in the event of third-party failure.</td>
</tr>
<tr>
<td></td>
<td>• Decreased dependency on homogeneous physical assets</td>
<td>• Data recovery testing must be conducted periodically to validate that backup procedures and media work as expected.</td>
</tr>
<tr>
<td></td>
<td>• Increased dependency on Internet access</td>
<td>• DRPs that rely entirely on cloud computing must be tested periodically to ensure effectiveness.</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>• Increased reliance on third-party cloud service providers</td>
<td>• The enterprise should limit vendor selection to reputable cloud service providers able to demonstrate robust DR capabilities.</td>
</tr>
<tr>
<td></td>
<td>• Loss of direct control over IT processes</td>
<td>• The necessary controls (encryption) should be implemented to protect data backed up/stored in the cloud.</td>
</tr>
<tr>
<td></td>
<td>• Increased reliance on third-party recovery capabilities</td>
<td>• BIA for critical functions must be conducted before deciding to migrate to a cloud provider to assess the risk and define BCM requirements.</td>
</tr>
<tr>
<td></td>
<td>• Increased agility and flexibility to move applications between different resources</td>
<td>• Contracts and SLAs should include clear BCM requirements.</td>
</tr>
<tr>
<td></td>
<td>• Increased flexibility to adjust capacity during higher or lower demand times</td>
<td>• BCM testing should include services provided by cloud vendors.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• BaaS, DRaaS and STaaS should be tested periodically to validate that data can be restored within the RTO and RPO.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In-house backups for critical data must be continued to ensure recovery in the event of third-party failure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data recovery testing must be conducted periodically to validate that backup procedures and media work as expected.</td>
</tr>
</tbody>
</table>

**Figure 1—BCM Strategy Considerations (cont.)**
## Business Continuity Risk Management and Governance Considerations

Enterprises must develop an appropriate BCM program to determine and address their own BC needs, and in some cases to also comply with laws and regulations that require proper planning to minimize the effects of disruptive events. Industries such as financial services, healthcare and government agencies are mandated to implement and maintain BCM programs to ensure that critical data are available at all times. Failure to implement the necessary processes to address disruptive events can result in penalties, even if the enterprise is not obligated to meet a particular regulatory requirement for BCM. Internal or external SLAs or contractual obligations may include clauses related to availability service levels or production commitments that should be maintained.

Ongoing management of the BCM program ensures that information used to direct BCM efforts is current, thus reducing the need for a “big bang” BIA update once a year. Just as business and technology change constantly so do BCM plans and strategies. Enterprise and IT change management policies and procedures should include risk assessment steps that provide the necessary input to keep BCM plans current and relevant.

When major technology changes occur within the enterprise, BCM documentation must be updated to account for new risk, threats and actions needed to minimize disruption of business operations. Technology advances can become a new risk (e.g., proliferation of laptop computers, tablets, smart phones, web-based applications and mobile apps), but also can provide new continuity capabilities (e.g., higher capacity backup tapes, disk mirroring capabilities, greater bandwidth, faster communication channels, remote erase capabilities, remote access to enterprise resources) and both effects must be considered and incorporated into BCM documentation.

---

### Figure 1—BCM Strategy Considerations (cont.)

<table>
<thead>
<tr>
<th>Area of Consideration</th>
<th>Impacts</th>
<th>BCM Strategy Considerations</th>
</tr>
</thead>
</table>
| **Mobile devices**    | • Increased prevalence of mobile devices in the work space  
                        • Increased reliance on technology to maintain productivity  
                        • Improved access to remote processes and workflow capabilities  
                        • Real-time reporting of events (positive and negative)  
                        • Increased presence of externally owned devices (a practice known as bring your own device or BYOD) by employees or suppliers accessing the network for information | • BCM plans should include mobile devices supporting critical functions.  
• Mobile devices supporting critical functions should be backed up periodically.  
• BCM training and awareness should include information on how to back up mobile devices that are used for business purposes.  
• BCM communication plans should leverage the proliferation of mobile devices and use multiple types of communication methods during a crisis (voice, text, social networks).  
• Contracts with mobile device vendors should include BCM requirements that specify how fast lost/stolen/destroyed devices must be replaced.  
| **Social networks**    | • Increased publicity and awareness of the variety of events that can affect business operations  
                        • Real-time reporting of events  
                        • Faster publication of high-profile incidents | • BCM should include policies and procedures that define proper use of social networks during crisis, including a list of approved sites and approved spokespersons.  
• Using social networks during crisis to communicate instructions or provide status reports should be limited to personnel qualified to communicate on behalf of the enterprise.  
• BCM training and awareness should include information regarding proper use of social networks during a crisis.  

---

**Business Continuity Risk Management and Governance Considerations**

Enterprises must develop an appropriate BCM program to determine and address their own BC needs, and in some cases to also comply with laws and regulations that require proper planning to minimize the effects of disruptive events.
**Risk Management**

Lost revenue, economic penalties, lost competitive advantage and reputational damage are some of the risk consequences that the enterprise must address by implementing a business strategy that includes an effective BCM program. Senior management must complete periodic risk analysis for critical functions and associated processes to identify likely risk events and their impact on operations. The analysis must be updated as business processes, organizations and IT systems change; in particular, risk analysis must be performed as the enterprise considers:

- Major organizational changes, such as acquisitions, expansions and restructuring
- Major technology changes, such as enterprise software implementations, adoption of virtualization, cloud computing and advance data storage
- Geographic changes, such as relocation, collocation and offshoring

BIA is the primary BCM component used to identify the business processes that must be restored immediately after a business disruption or disaster and the order in which these processes must be restored to full functionality. The level of complexity to map applications and services to business processes to facilitate an effective BIA represents a challenge for many enterprises, especially for those adopting some of the emerging technologies described in this document. As a result, special consideration should be given to the BIA process and, if necessary, enterprises must refine the frequency and depth of the BIA.

**Governance**

Management support is fundamental to the success of an effective BCM program. If leadership by senior management and board oversight are lacking, the appropriate focus, priority and resources may not be devoted to the program. Adequate policies requiring management to implement and maintain a BCM program to sustain business availability should be part of enterprise governance to ensure that efforts are effectively managed. Proper governance over BCM may increase the synergy among groups supporting different elements of the program (e.g., incident management, crisis and emergency response and disaster recovery). Governance over BCM efforts helps coordinate efforts and communicate roles and responsibilities to all stakeholders.
**Business Continuity Management: Emerging Trends**

Figure 2 provides a RACI chart for the key governance and management practices necessary to enable BCM.

<table>
<thead>
<tr>
<th>Figure 2—BCM Key Governance and Management Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Governance Practice</strong></td>
</tr>
<tr>
<td>EDM03.01 Evaluate risk management.</td>
</tr>
<tr>
<td>EDM03.02 Direct risk management.</td>
</tr>
<tr>
<td>EDM03.03 Monitor risk management.</td>
</tr>
<tr>
<td><strong>Key Management Practice</strong></td>
</tr>
<tr>
<td>DSS04.01 Define the business continuity policy, objectives and scope.</td>
</tr>
<tr>
<td>DSS04.02 Maintain a continuity strategy.</td>
</tr>
<tr>
<td>DSS04.03 Develop and implement a business continuity response.</td>
</tr>
<tr>
<td>DSS04.04 Exercise, test and review the BCP.</td>
</tr>
<tr>
<td>DSS04.05 Review, maintain and improve the BCP.</td>
</tr>
<tr>
<td>DSS04.06 Conduct continuity plan training.</td>
</tr>
<tr>
<td>DSS04.07 Manage backup arrangements.</td>
</tr>
<tr>
<td>DSS04.08 Conduct post-resumption review.</td>
</tr>
</tbody>
</table>

Legend: R=Responsible, A=Accountable, C=Consulted, I=Informed

Source: COBIT 5 Enabling Processes, EDM03 and DSS04 RACI charts

### Assurance Considerations

The primary assurance consideration related to business trends and emerging technologies and its impact on continuous operations is: Ascertain whether the enterprise has a mature process to assess risk related to changes and properly modify BCM (BC, DR, CM, incident response) strategies accordingly.
As an enterprise’s vision and strategy change over time, it is important for assurance professionals to remain current on the various standards (e.g., ISO, NIST), frameworks (e.g., COBIT 5) and best practices that address BCM. These materials provide good references to support the establishment, maturity and assessment of specific BCM capabilities. Specific examples of these are:

- Standards such as:
  - International Organization for Standardization (ISO) 22301, formerly BS25999—Business Continuity Management
  - ISO/PAS 2239:2007—Guideline for incident preparedness and operational continuity management
  - Federal Financial Institutions Examination Council (FFIEC)—BCP Examiner’s Handbook
  - National Institute of Standards and Technology (NIST) SP800-30 Rev 1—Guide for Conducting Risk Assessments
  - NIST 800-34 Rev 1—Contingency Planning Guide for Federal Information Systems

- Frameworks such as:
  - ISACA—COBIT 5, Val IT and Risk IT
  - The commercially developed Business Continuity Maturity Model (BCMM) for assessing state of preparedness
  - IT Infrastructure Library (ITIL)—Guidelines for The Business Continuity Planning Process and Documentation

- Best practices such as:
  - Business Continuity Institute (BCI)—Business Continuity Management-Good Practice Guidelines
  - Disaster Recovery Institute (DRII)—Business Continuity Planning Professional Practices
  - European Network and Information Security Agency (ENISA)—Business Continuity Management & Resilience

Assessing the enterprise’s current capabilities and identifying improvements needed to reach or maintain the desire level of maturity are critical tasks for assurance organizations. COBIT 5, Risk IT and Val IT can be used jointly to provide decision makers with a set of criteria for assessing the value created through the delivery of a high-quality BCM program. These frameworks can help answer strategic questions, including the following:

- Are we doing the right things?
  - What is our industry doing with respect to continuity management over emerging business trends and technologies and how is our enterprise placed in relation to our peers?

- Are we getting the benefits?
  - Based upon these comparisons, is our BCM providing competitive advantage?

- Are we doing them the right way?
  - How do we identify what is required to reach additional levels of cost-effective availability and business resiliency through future-state BCM strategies?

- Are we getting them done well?
  - How do we assess the level of maturity of our BCM program and supporting processes?

**BCM Assurance Framework**

The objectives of a continuity assurance review should be to provide management with:

- An evaluation of a business unit readiness in the event of a disruption
- A list of issues that may limit interim business processing and restoration after a disruption
- An independent analysis of the effectiveness of the continuity plan
COBIT® 5: Enabling Processes and the IT Continuity Planning Audit/Assurance Program from ISACA provide a comprehensive guide to the assurance professional to plan and execute a business continuity assessment. Specific guidance on BCM is provided in the following COBIT 5 enabling processes:

- EDM03 Ensure Risk Optimisation—Determine whether IT risk appetite is commensurate with business objectives and enterprise risk tolerance
- APO02 Manage Strategy—Determine whether the IT strategy is aligned with business objectives
- APO09 Manage Service Agreements—Determine whether IT services and service levels meet current and future enterprise needs
- APO10 Manage Suppliers—Determine whether IT has processes to minimize risk associated with non-performing suppliers
- APO12 Manage Risk—Determine whether the IT strategy supports business requirements to comply with external laws and regulations
- BAI04 Manage Availability and Capacity—Determine whether IT has the necessary processes to predict performance and capacity requirements to maintain availability
- BAI06 Mange Changes—Determine whether risk associated with IT changes is properly assessed and reflected in the continuity strategy
- DSS04 Manage Continuity—Determine whether appropriate plans exist to enable the business and IT to respond to incident and disruptions in order to continue operations of critical business functions

Conclusion

BCM must continue to evolve as business practices and emerging technologies continue to shape the business landscape. Greater customer expectations and increased regulatory and legal requirements for availability and continuity cannot be ignored. BCM should be integrated into enterprise strategic planning to ensure proper alignment to meet market demands and regulatory requirements. Emerging technologies supporting business processes can also be leveraged to improve BCM and reduce cost. Virtualization, cloud computing, mobile devices and social networks are examples of emerging technologies that can be leveraged to improve BCM. However, without proper business alignment, risk management and governance, BCM may not be able to exploit the potential benefits of using emerging technologies. Enterprises should not allow the BCM program to stagnate; continuous improvement through regular reviews, testing and updates should be just as critical as the initial development and implementation to ensure that changes in the business landscape and technology advances are incorporated properly to minimize risk and realize benefits.

Additional Resources and Feedback
Visit www.isaca.org/Business-Continuity for additional resources and use the feedback function to provide your comments and suggestions on this document. Your feedback is a very important element in the development of ISACA guidance for its constituents and is greatly appreciated.