Gartner Research

Publication Date: 16 February 2010 ID Number: G00174455

Activity Cycle Overview: Business Continuity Manager Role, 2010 to 2011

Roberta J. Witty

There are many standards and frameworks to which organizations can turn to develop their business continuity management (BCM) programs. Business continuity managers and other enterprise stakeholders can apply the Gartner BCM Activity Cycle model — regardless of the selected standard or framework — to their own programs to ensure that they are mature, effective and consistently implemented.

Key Findings

- The practice of IT disaster recovery management (IT DRM) is well-established and widely recognized for its importance to the business. Therefore, management attention to recovery is taking on a wider scope of ensuring that the operations of the entire business can effectively be recovered in case of a disruptive event.
- Many BCM professionals are new to the role, or have made the transition from the IT DRM program; thus, they do not have a business-oriented view of operational continuity.
- Building a BCM program is complicated by the enterprisewide scope of the effort.
- Enterprise efforts to improve business resilience can affect virtually all business processes, and these changes must be integrated with the daily management of business operations processes.

Recommendations

BCM professionals should:

- Use the Gartner BCM Activity Cycle process, regardless of the standard or framework they may already be using, to perform a readiness recovery check and a gap analysis on their BCM program's detailed activities.
- Build a three-year BCM road map and an annual implementation plan to close the gaps in existing recovery capabilities. Review the road map and implementation plan with management to secure appropriate funding for program enhancements.
- Review vendor product and service offerings to see how they map to the Gartner BCM Activity Cycle, the International Organization for Standardization's Plan-Do-Check-Act (ISO's PDCA) model, and the Core Program Elements Using a Process Approach (in Figure 1) of the Sloan report titled, "Framework for Voluntary Preparedness." Also review these offerings to see how they fit into the entire life cycle of a BCM program. Such mapping can also help determine which parts of vendor product and service offerings would benefit from more attention to product/service development.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ANALYSIS

1.0 Introduction

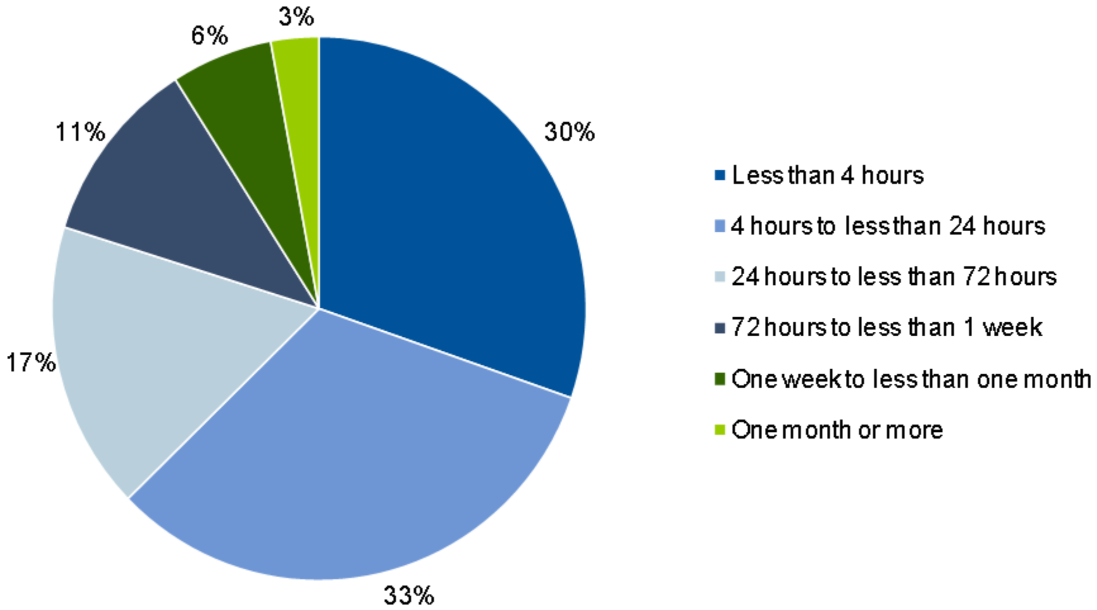
IT DRM is a well-established discipline, but BCM (see Note 1) remains a new and less well-understood area for many organizations (see "Business Continuity Management Defined, 2008"). Many managers who are responsible for ensuring the continuity of business operations are challenged in knowing how to start a BCM program, and, more importantly, how to maintain it over time. They recognize that the risks to the operational continuity of their enterprises are increasing, influenced by factors including globalization and the 24/7 nature of business. They also know that they must make the transition from traditional IT DRM to a "business centric" approach, but they do not know how to do so.

Building a successful BCM program is complicated for a number of reasons:

- It must be enterprisewide in scope and implementation practices. For example, an availability vulnerability in one location might impact many others, and many business units. Therefore, risk assessments must be conducted to identify availability vulnerabilities in each location; business impact analyses must be conducted to determine the impact of these vulnerabilities on and across business processes; resource allocation challenges must be addressed (work might need to be rerouted to other operating locations); and an enterprisewide metrics and reporting system must be developed and the results communicated to all appropriate stakeholders.
- It requires participation from all lines of business and all internal organizations to be effective.
- The different — and competing — recovery priorities of the various stakeholders can be difficult to reconcile. For example, the business continuity manager must determine who pays for what part of a shared recovery solution, or must reconcile the opinion that his or her operations are more important than someone else's.
- Some managers may fall victim to the "nothing has happened yet" mind-set, and believe that they are invulnerable.
- A broad range of BCM regulations, standards and frameworks (see Note 2) need to be navigated, especially in enterprises with complex or international operations.
- BCM costs money, and many business managers view it as an expensive "insurance policy" that they may never need.
- Moreover, when BCM is done correctly, it requires extensive integration with business operations management, which can radically change business practices.

Despite these obstacles, enterprises increasingly recognize that an effective BCM program is absolutely critical to their operations. As Gartner's 2010 Risk and Security Survey shows (see Figure 1), recovery time objectives (RTOs) continue to fall, getting closer to the time of the disaster event, which means that recovery of the business or IT operation must be done more quickly — and this can only occur if advance planning is in place.

Figure 1. Business Functions and RTOs — Gartner's 2010 Risk and Security Survey



N=133

Source: Gartner (February 2010)

Enterprises that do not have an appropriate BCM program in place in a time of crisis may create a series of consequences — such as damaged profitability, competitiveness and reputation — that ultimately result in business failure. For this reason, the time to build a BCM program is *not* while responding to a crisis, when it is too late, but rather *before* disaster strikes. This makes it possible to identify and prioritize needed resources, procure them at the best possible price and plan their use well in advance of an emergency.

2.0 Current and Future Outlook

The role of the business continuity manager is to manage the overall enterprise BCM program by coordinating and consolidating information gathered from all lines of business, departments and external resources to ensure that the following activities are completed:

- Developing a vision, scope, policy, principles and standards to guide the BCM program
- Defining the environment in which the enterprise operates, including:
  - Internal and external relationships (for example, with employees, independent contractors, business partners, suppliers and government agencies)
  - Industry type
  - Contractual obligations
  - Regulatory mandates
- Documenting critical business functions (key resources, infrastructure, tasks and responsibilities) and their recovery requirements

- Documenting the business value and cost of downtime for each critical business function
- Developing a business and technical recovery strategy for critical business functions
- Defining and implementing response, recovery and restoration plans
- Developing confidence in, and awareness of, plans and solutions through awareness, training and exercising activities
- Keeping recovery plans up to date
- Executing response, recovery and restoration plans in the event of a crisis
- Addressing program governance issues

These responsibilities can be categorized in the four phases of the Gartner BCM Activity Cycle.

3.0 The Gartner BCM Activity Cycle

This is a program management methodology that can be used to increase the maturity of an enterprise's BCM program, regardless of the industry or country regulations, standards or frameworks currently being used by the organization. The Gartner BCM Activity Cycle was developed in response to strong client demand for help in developing successful BCM programs that are capable of maturing over time. In the past, BCM programs tended to focus strictly on the "doing" component — building and exercising plans — and did not address program management activities that can help program managers secure needed resources before the "doing" starts. If you are using another methodology, then the Gartner BCM Activity Cycle can be used as a cross-check to ensure that all BCM components and practices are covered under your current approach.

Govern: Governance means specifying the decision-making authority and accountability for the encouragement of desirable behaviors. For BCM professionals, this phase involves establishing a decision-making authority and accountability framework that is used on an ongoing basis to address the risks of business and IT interruption, and the resulting effects on each line of business or department, each physical facility and the enterprise as a whole.

Plan: Planning, in the generic sense, involves developing a consistent strategic and organizational model that will drive effective tactical and annual plans. For BCM professionals, this phase involves making the business case for BCM through the use of key performance indicators and key availability risk indicators (see "A New Approach: Obtain Business Ownership and Investment Commitment for Business Continuity and Resilience Management Through Key Performance and Risk Indicator Mapping"); setting up the key BCM program structures; and defining vision, scope, objectives, roles and responsibilities, organizational and industry continuity-of-operations drivers, long-term road maps, and budget plans that are aligned with the business.

Build: Building involves the development of architecture, controls and process formalization as strategic initiatives. For BCM professionals, this phase involves developing policies, principles and standards, as well as a process and control framework to assess, measure, communicate and report on five of the six components of the BCM program (pandemic planning is not covered in this version of the Gartner BCM Activity Cycle — see "Business Continuity Management Defined, 2008").

Run: Running, as a generic activity, includes the execution, implementation and operation of the controls, methodologies and strategies developed in prior phases. For BCM professionals, this phase involves implementing, exercising and maintaining all processes and controls established in the build phase — including the development and implementation of recovery technologies, services and plans — as well as executing the recovery plans when necessary. This phase also includes a review cycle of the entire set of Gartner BCM Activity Cycle constructs and activities to ensure that they reflect the current state of the business and the marketplace.

4.0 The Gartner BCM Activity Cycle Phase Comparison to BS 25999 and the Sloan Report: "Framework for Voluntary Preparedness"

To better enable our readers to use and understand the Gartner BCM Activity Cycle, Table 1 provides a comparison of its phases to those in two well-known BCM frameworks: BS 25999, which is based on the ISO's PDCA, and the Core Program Elements Using a Process Approach (in Figure 1) of the Sloan report titled, "Framework for Voluntary Preparedness."

Table 1. Comparison of the Gartner BCM Activity Cycle to the ISO's PDCA/BS 25999 and the Core Program Elements Using a Process Approach (in Figure 1) of the Sloan Report, "Framework for Voluntary Preparedness"

Gartner	ISO/BS 25999	Sloan Report: "Framework for Voluntary Preparedness"	Method Comparison
Govern	Plan Check Act	Program Policies and Procedures Review, Maintenance, Improvement	Gartner's Govern phase specifically calls out governance as a crucial activity in managing any critical organizational program, including ongoing program alignment to business needs, which can then lead to actions that update all activities and outcomes of the Plan, Build and Run phases. In the ISO's PDCA/BS 25999 model, BCM program governance is addressed in Section 3.2: "Establishing and Managing the BCMS," Section 5: "Monitoring and Reviewing the BCMS," and Section 6: "Maintaining and Improving the BCMS." In the Sloan report's "Framework for Voluntary Preparedness" Core Program Elements model, program governance is addressed in the "Program Policies and Procedures" and "Review, Maintenance, Improvement" elements.
Plan	Plan	Program Policies and Procedures Analysis	Gartner's Plan phase is focused on program scope and management, and activities. In the ISO's PDCA/BS 25999 model, BCM program planning activities are covered in Section 1: "Scope" and Section 3: "Planning the Business Continuity Management System." In the Sloan report's "Framework for Voluntary Preparedness" Core Program Elements model, BCM program planning activities are covered as follows: • Policy Statements and Roles and Responsibilities are covered in the Program, Policies and Procedures element. • Analysis of legal and other requirements is covered in the Analysis element.

Gartner	ISO/BS 25999	Sloan Report: "Framework for Voluntary Preparedness"	Method Comparison
Build	Plan Act	Program Policies and Procedures	Gartner's Build phase is focused on building the BCM architecture and program practices. In the ISO's PDCA/BS 25999 model, BCM architecture activities are covered in the Plan phase. In the Sloan report's "Framework for Voluntary Preparedness" Core Program Elements model, building the BCM program architecture is covered in the Program Policies and Procedures element.
Run	Do Check Act	Analysis Planning Implementation and Operational Controls Checking and Evaluation Review, Maintenance, Improvement	Gartner's Run phase covers the implementation and ongoing operation of the BCM program, including program monitoring; status reporting; maintaining and improving the BCM plans, practices and overall program; and the execution of recovery plans, if needed. In the ISO's PDCA/BS 25999 model, the implementation and operation of BCM program activities are covered in Section 4: "Implementation and Operation of the BCMS," Section 5: "Monitoring and Reviewing the BCMS," and Section 6: "Maintaining and Improving the BCMS." (In the ISO's PDCA model, they are divided into Check and Act phases.) In the Sloan report's "Framework for Voluntary Preparedness" Core Program Elements model: • Conducting risk assessments, impact analyses, criticality analyses and resource analyses is covered in the Analysis element. • All other implementation and operation activities are covered in the Planning, Implementation and Operational Controls, Checking and Evaluation, and Review, Maintenance, Improvement elements.

Source: Gartner (February 2010)

After comparing these three methods, you will see that the Gartner BCM Activity Cycle takes a program management and governance focus — with the Govern, Plan and Build phases covering those activities and the Run phase covering the program execution activities; whereas the ISO and Core Program Elements phases are more aligned to program execution with one phase — the Plan phase for ISO — and two phases — Program Policies and Procedures and Review, Maintain, Improvement for Core Program Elements.

If you are obtaining certification under BS 25999-2 (for Voluntary Private Sector Preparedness Accreditation and Certification [PS-Prep] or not), then you must show that you are in compliance with that standard. If you are obtaining certification under the other standards for PS-Prep (yet to be confirmed), then you will have to show conformance to them. In any case, regardless of whether you are obtaining BCM program certification, the Gartner BCM Activity Cycle can be used to ensure that your program components and activities are complete.

5.0 The Gartner BCM Activity Cycle's Detailed Activities

This section outlines the detailed activities in each phase of the Gartner BCM Activity Cycle. As your BCM program progresses, the status and outputs of each activity should be monitored, reviewed and updated based on prior results, as well as reported to management to show overall program success or failure. The results of each Gartner BCM Activity Cycle phase should be used as input to the other phases to ensure that the management of the BCM program, as well as all recovery plans and solutions, is kept current. Ensuring that this review and updating process is in place is the responsibility of the business continuity manager.

5.1 Phase 1: Govern

BCM professionals must work closely with senior executives, line-of-business managers, the IT organization, the risk management organization, and other internal and external stakeholders to establish an effective decision-making authority and accountability framework. This framework will ensure that business interruption risks are appropriately identified, assessed, mitigated and reported to all stakeholders. The key activities of this phase include the development of:

- A BCM steering committee comprising senior management from each line of business
- An organizational charter that maps out the accountability framework for the BCM program
- Program maturity assessment metrics and methodologies to track program status, and to improve overall program maturity on an ongoing basis
- A review and update process and feedback methodology to ensure that the BCM program aligns with business practices and changing priorities

5.2 Phase 2: Plan

BCM professionals must develop a BCM program structure that is aligned with the business context, taking into account strategic, operational, regulatory, relationship and other requirements. The key activities of this phase include the development of:

- The BCM program's vision, scope and objectives
- Key stakeholder identification, including personnel from all lines of business, IT, human resources, corporate communications/public relations, legal, compliance, auditing, privacy, risk management, facilities management, physical security and safety organizations, and external authorities, emergency organizations, customers, trading partners and suppliers
- Roles and responsibilities, including skills/competencies and certification requirements, of the BCM and IT DRM program offices, as well as recovery team representation from the lines of business and other internal departments
- A communication program for the business value of BCM
- A five-year strategic road map
- An annual implementation plan
- An annual financial analysis and budget

5.3 Phase 3: Build

BCM professionals must develop policies, principles and standards, as well as a process and control framework, to assess, measure, communicate and report on the six components of the BCM program. The key activities of this phase include the development of:

- BCM policies, principles and standards

- An inventory and interdependency map of critical business processes, facilities, resources and assets, as well as those of key public and private partners
- An inventory of BCM-related standards, contracts and government regulations that impact the enterprise and the industry in which it operates
- A BCM framework and methodology to ensure the consistency of implementation across all lines of business
- A business interruption risk assessment methodology
- An external service provider business interruption risk assessment methodology
- A business impact analysis (BIA) methodology
- A BCM training and awareness methodology
- A plan exercise methodology
- A management status reporting and communications methodology
- Technology selection for BCM program management

5.4 Phase 4: Run

BCM professionals must work with a broad range of stakeholders to ensure that the enterprise's BCM and IT DRM strategies (including workforce, facilities, business processes and infrastructure, IT process and infrastructure, suppliers, partners, customers, and finances), plans, and solutions are in place, and aligned with current and changing business needs. The key activities of this phase include the development, implementation, management, exercising, maintenance and execution of the following.

5.4.1 BCM Program Management

- BCM/IT DRM role and responsibility rollout, training, and competency testing
- BCM planning software
- Audit request management from internal and external auditors, as well as prospects and customers, as to the status of the BCM program
- Reporting to management, auditors and regulators on the status of BCM program activities
- The organizational BCM external certification process, if such certification is being attained
- Financial reporting requirements

5.4.2 Assessment and Analysis

- A maturity self-assessment
- A business interruption risk assessment, at least on an annual basis
- A BIA for each line of business and department, at least on an annual basis

- A business interruption risk assessment, at least on an annual basis, of all external service providers — e.g., business process, IT and recovery service providers
- RTOs, recovery point objectives and the maximum tolerable period of downtime
- A prioritization schedule of availability requirements based on the results of the risk assessment and the BIA

5.4.3 Crisis/Incident Management

- A damage assessment strategy and supporting operational plans
- A life and safety strategy and supporting operational plans
- A crisis/incident management strategy and supporting operational plans
- A crisis communications strategy and supporting operational plans
- An emergency notification strategy and supporting operational plans
- A community outreach, support and assistance strategy, and supporting operational plans
- A crisis management team
- A crisis management/emergency operations center
- A crisis communications team
- Formal disaster declaration procedures
- Damage assessment arrangements
- Life and safety arrangements
- Crisis/incident management arrangements
- Crisis communications arrangements
- BCM partnerships with government authorities, public authorities and industry associations
- Incident management software/services
- Emergency notification software/services

5.4.4 Business Recovery

- A records retention strategy
- A business recovery strategy
- A supply chain recovery strategy
- Business operations risk mitigation controls
- Knowledge management systems to automate enterprise "historical knowledge"
- Work area recovery arrangements for business personnel

- Procedural records retention arrangements
- Business resumption plans by line of business and department (including the need for new application development as well as linkages to IT DRM plans)
- Business response, recovery and restoration plans by line of business and department (including linkages to IT DRM plans)
- Telework arrangements
- Workforce continuity arrangements
- Supply chain recovery arrangements
- Business interruption insurance coverage
- Business response, resumption, recovery and restoration plan maintenance according to the results of plan exercises, and business and IT changes, at least on an annual basis, or when a major change occurs

5.4.5 IT Recovery

- A technical recovery strategy
- IT DRM technology selection
- IT operations recovery risk mitigation controls
- Work area recovery arrangements for technical personnel
- Data center (network, hardware, software and data) backup and recovery arrangements
- Information security solution recovery arrangements, such as key management, authentication, access control and so on
- Telephony recovery arrangements
- Telework arrangements
- Records retention and archival arrangements
- New application support for business resumption procedures (by line of business and department)
- IT operations response, recovery and restoration plans (including linkages to business recovery plans)
- IT operations recovery response, recovery and restoration plans, updating and maintenance according to the results of plan exercises, and business and IT changes, at least on an annual basis, or following the implementation of major changes to production

5.4.6 Awareness, Training and Exercising

- Workforce BCM awareness training programs
- Business response, resumption recovery and restoration plan exercises
- Technical response, resumption recovery and restoration plan exercises

5.4.7 BCM Program Maintenance

- A review of all program components (e.g., charter, policy, expectations, legal/regulatory requirements, resources and so on) to ensure that they align with current business availability needs
- A review of all program practices (e.g., risk assessment, BIA, plan management, crisis/incident management, exercising and so on) to ensure that they align with current BCM market practices
- A review of all risk assessment outcomes and BIA outcomes to ensure that they align with current business availability needs
- A review of all exercise results
- A gap analysis and closure schedule for all program nonconformities
- An update of all BCM program components and practices
- An update of all business and IT recovery strategies and solutions
- An update of all recovery plans

5.4.8 BCM Program Execution During a Crisis

- Crisis/incident management plans
- Crisis communications plans
- A damage assessment
- Life and safety checks
- Business response, resumption, recovery and restoration plan execution
- Technical response, resumption, recovery and restoration plan execution
- Postmortem review and follow-up management of plans and solutions after a crisis

RECOMMENDED READING

"Business Continuity Management Defined, 2008"

"Hype Cycle for Business Continuity Management, 2009"

"Gartner for IT Leaders Overview: The Business Continuity Manager"

"Toolkit: Job Description for Business Continuity Manager"

"Workforce Continuity Defined"

"Ten Remote-Access Failures Your Company Could Avoid in an Emergency"

"Personal Preparedness Enhances Corporate Recovery"

"Enlightening the CEO on Business Continuity Management"

"Banking and Investment Services BCM/DR, 2006"

"Business Continuity Planning for FSPs"

"Automated Emergency Notification Will Speed Disaster Recovery"

"Best Practices for Conducting a Business Impact Analysis"

"Research Roundup: Business Continuity Management and IT Disaster Recovery Management, 3Q09"

"Predicts 2009: Business Continuity Management Juggles Standardization, Cost and Outsourcing Risk"

"Predicts 2010: The Role of Business Continuity Management Continues to Expand and Extend"

"Predicts 2010: New IT Disaster Recovery Technologies Are Emerging, but Most Are in the Early Stages"

"MarketScope for Emergency and Mass Notification Services"

"Ten Best Practices for Creating and Maintaining Effective Business Continuity Management Plans"

"A New Approach: Obtain Business Ownership and Investment Commitment for Business Continuity and Resilience Management Through Key Performance and Risk Indicator Mapping"

"Business Continuity Management Key Initiative Overview"

"How to Organize for Disaster Recovery Management"

"Toolkit: 2009 BCM Program Overview"

Acronym Key and Glossary Terms

BCM	business continuity management
BCMS	BCM system
IT DRM	IT disaster recovery management

Note 1
BCM Definition

BCM is a process supported by senior management that is designed to coordinate, facilitate and execute activities that ensure effectiveness in:

- Identifying and mitigating operational risks before they occur
- Responding to disruptive events (natural and man-made, accidental and intentional)
- Recovering mission-critical business and IT operations after disruptive events
- Conducting a postmortem of an event to improve future recovery operations

BCM is composed of six major components (see "Business Continuity Management Defined, 2008"):

1. Crisis/incident management
2. Emergency response

3. IT DRM
4. Business recovery
5. Contingency planning
6. Pandemic planning

Note 2
BCM Regulations, Standards and Frameworks

The following are examples of BCM regulations, standards and frameworks. None are widely perceived as representing a complete set of best practices, and no commonly accepted, industry-neutral BCM version has emerged:

- ASIS International Business Continuity Guidelines (International)
- ANSI ASIS SPC.1-2009: Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements With Guidance for Use American National Standard
- Basel Capital Accord
- Business Continuity Institute (BCI) — The BCI Good Practice Guidelines (International)
- BSI Group — Business Continuity Management. Specification (BS 25999-2:2007; U.K.)
- BSI Group — Information and Communications Technology Continuity Management. Code of Practice (BS 25777:2008; U.K.)
- BSI Group — IT Service Continuity Management. Code of Practice (Publicly Available Specification [PAS] 77:2006; U.K.)
- Canadian Standards Association — Z1600 Emergency Management and Business Continuity Programs
- DRI International — Generally Accepted Practices for Business Continuity Practitioners (International)
- U.S. Expedited Funds Availability Act — 12 U.S.C. 4001-4010
- U.S. Federal Financial Institutions Examinations Council (FFIEC) — Business Continuity Planning IT Examination Handbook: March 2008
- HB 221:2004 — Business Continuity Management Handbook (Australia)
- HB 292:2006 — A Practitioner's Guide to Business Continuity Management (Australia)
- ISO/PAS 22399:2007: Societal Security — Guideline for Incident Preparedness and Operational Continuity Management
- ISO 22301: Societal Security — Preparedness and Continuity Management Systems — Requirements
- ISO/IEC 27001:2005 — Information Technology — Security Techniques — Information Security Management Systems — Requirements
- IT Infrastructure Library (ITIL) v.3 (International)

- Monetary Authority of Singapore — Business Continuity Management Guidelines
- U.S. National Fire Protection Association (NFPA) 1600 — Standard on Disaster/Emergency Management and Business Continuity Programs (2007 Edition)
- U.S. National Institute of Standards and Technology (NIST) — Special Publication 800-34
- North American Electric Reliability Corporation (NERC) — Critical Infrastructure Protection Cyber Security Requirement 009
- Prudential Standard APS 232 — Business Continuity Management (Australia)
- Singapore Standard SS 507:2004 — Business Continuity/Disaster Recovery Service Providers
- SPRING Singapore Technical Reference (TR) 19:2005 — Business Continuity Management
- U.S. Public Law 110-53 — Implementing Recommendations of the 9/11 Commission Act of 2007, Title IX, Private Sector Preparedness

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509