IT Audit

Jean-Pierre Garitte

Antwerp, 5 June 2018

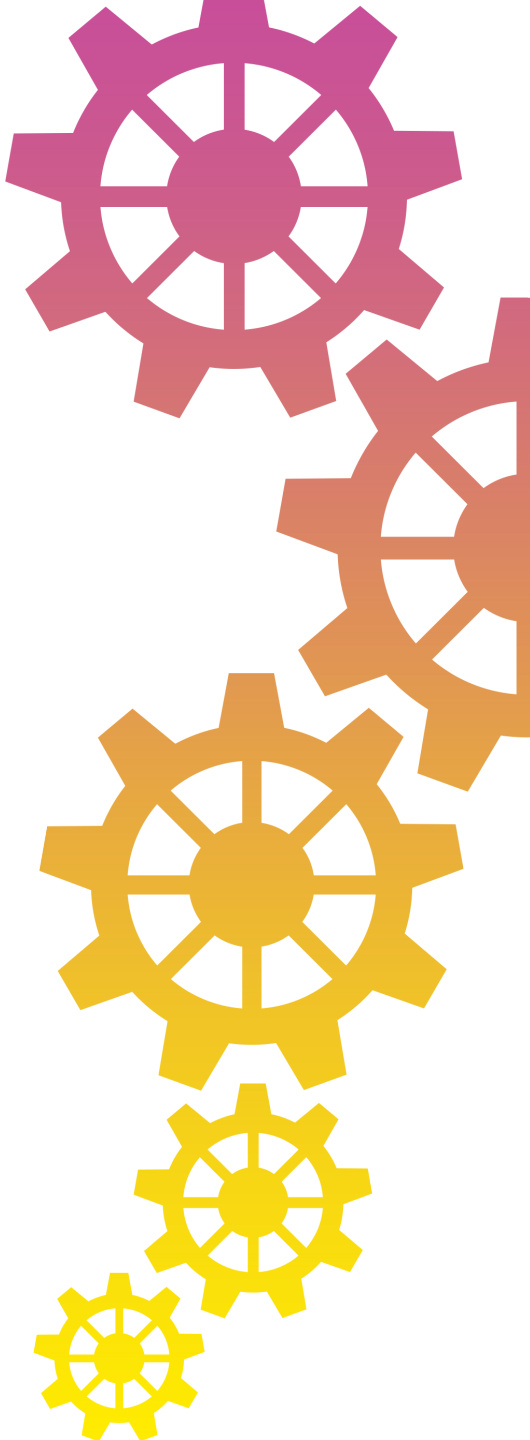
Internal Audit Training of Trainers

CFRR
Centre for Financial Reporting Reform
WORLD BANK GROUP
Governance

SAFE
Strengthening Accountability and the Fiduciary Environment

Co-funded by
European Union
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The IIA on IT audit



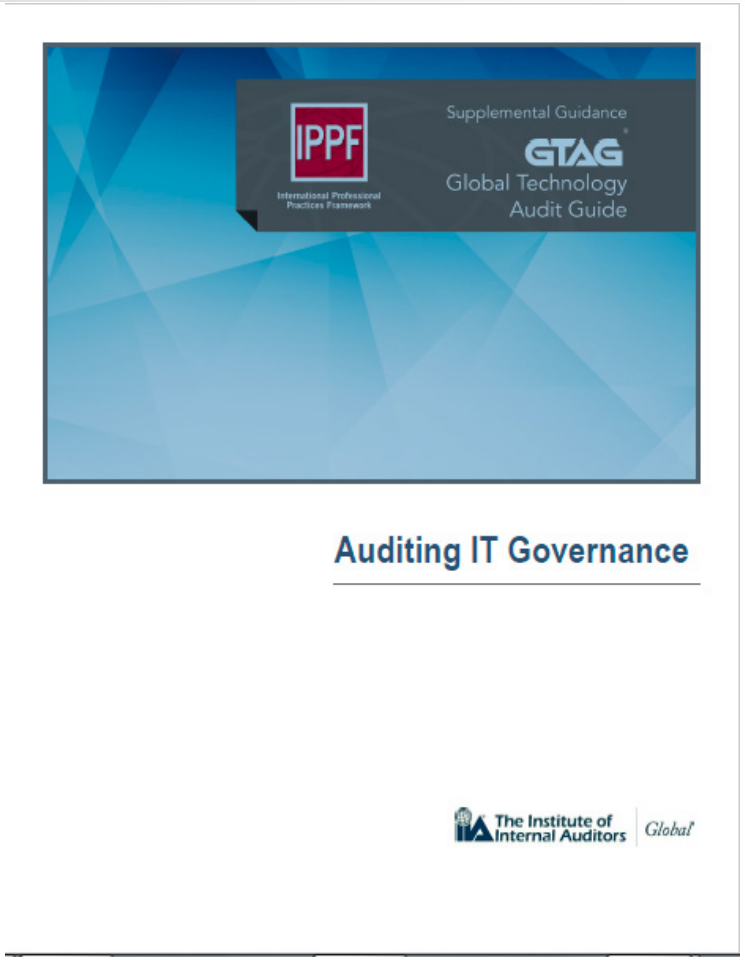
IIA Standard 1210 – Proficiency

Implementation Standard 1210.A3

Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

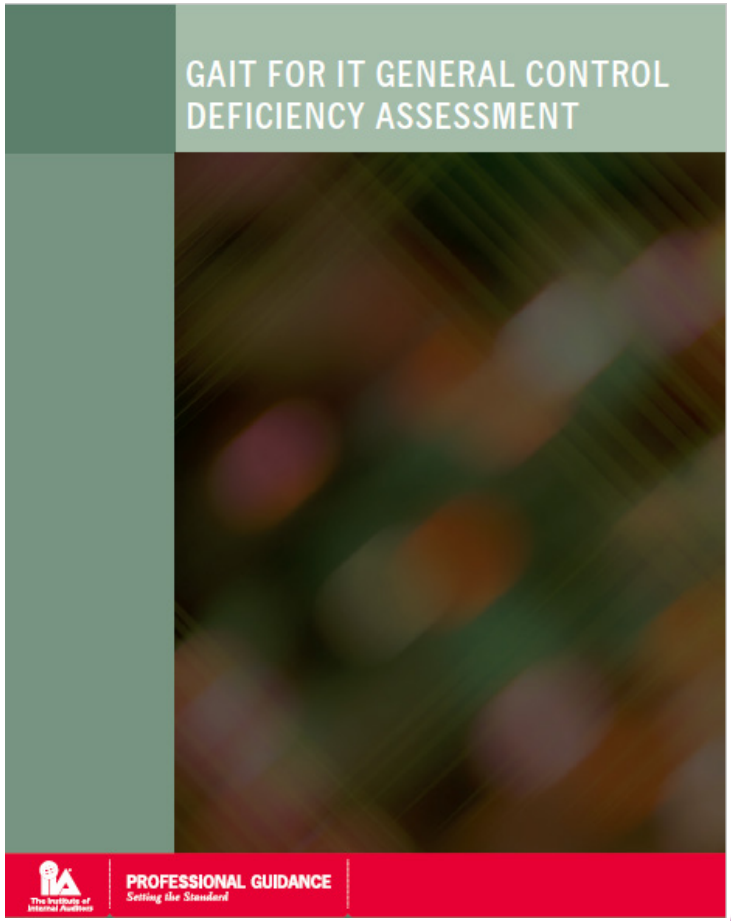
IIA Supplemental Guidance

- Practice Guides — GTAG®
- Global Technology Audit Guide (GTAG)

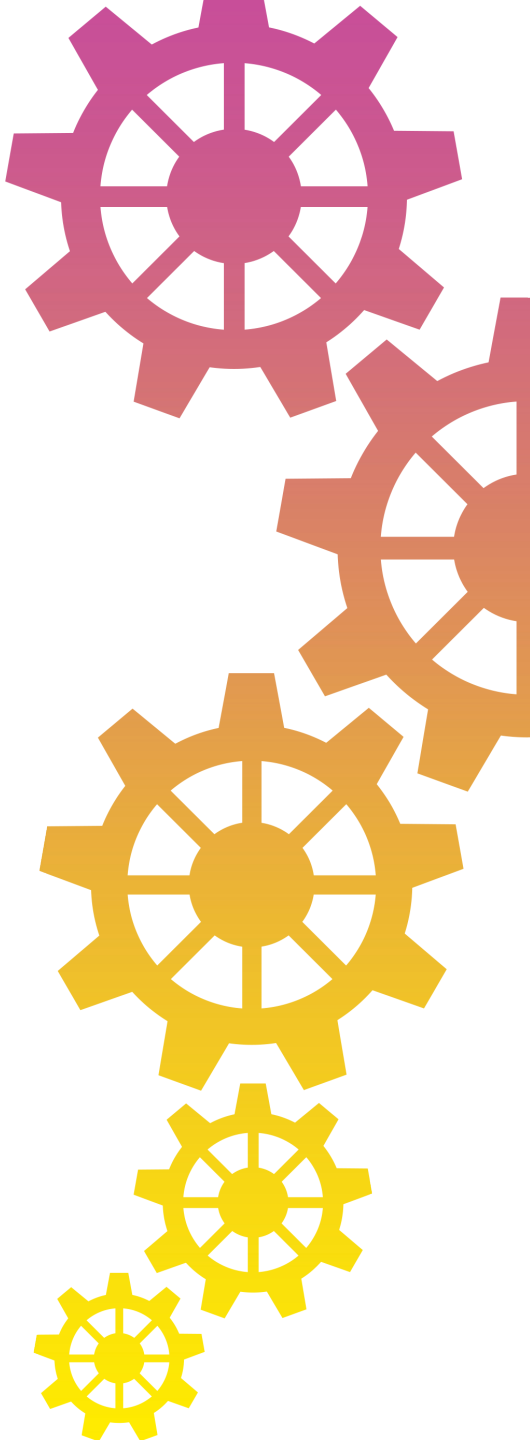


IIA Supplemental Guidance

- Practice Guides — GAIT
- Guide to the Assessment of IT Risk (GAIT)



The COBIT framework



The COBIT framework

What is the COBIT framework?

COBIT (Control Objectives for Information and related Technology) defines IT activities in a generic process model within four domains. These domains are:

» Plan and Organize

» Acquire and Implement

» Deliver and Support

» Monitor and Evaluate

The domains map to IT's traditional responsibility areas of plan, build, run and monitor.

Domain 1. Plan and Organize (PO)

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realization of the strategic vision needs to be planned, communicated and managed. Finally, a proper organization as well as technological infrastructure should be put in place. This domain typically addresses the following management questions:

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?
- Does everyone in the organization understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?

Domain 1. Plan and Organize (PO)

PO1 Define a Strategic IT Plan
PO2 Define the Information Architecture
PO3 Determine Technological Direction
PO4 Define the IT Processes, Organization and Relationships
PO5 Manage the IT Investment
PO6 Communicate Management Aims and Direction
PO7 Manage IT Human Resources
PO8 Manage Quality
PO9 Assess and Manage IT Risks
PO10 Manage Projects

Domain 2. Acquire and Implement (AI)

To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives. This domain typically addresses the following management questions:

- Are new projects likely to deliver solutions that meet business needs?
- Are new projects likely to be delivered on time and within budget?
- Will the new systems work properly when implemented?
- Will changes be made without upsetting current business operations?

Domain 2. Acquire and Implement (AI)

AI1 Identify Automated Solutions

AI2 Acquire and Maintain Application Software

AI3 Acquire and Maintain Technology Infrastructure

AI4 Enable Operation and Use

AI5 Procure IT Resources

AI6 Manage Changes

AI7 Install and Accredit Solutions and Changes

Domain 3. Deliver and Support (DS)

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and the operational facilities. It typically addresses the following management questions:

- Are IT services being delivered in line with business priorities?
- Are IT costs optimized?
- Is the workforce able to use the IT systems productively and safely?
- Are adequate confidentiality, integrity and availability in place?

Domain 3. Deliver and Support (DS)

DS1 Define and Manage Service Levels

DS2 Manage Third-party Services

DS3 Manage Performance and Capacity

DS4 Ensure Continuous Service

DS5 Ensure Systems Security

DS6 Identify and Allocate Costs

DS7 Educate and Train Users

DS8 Manage Service Desk and Incidents

DS9 Manage the Configuration

DS10 Manage Problems

DS11 Manage Data

DS12 Manage the Physical Environment

DS13 Manage Operations

Domain 4. Monitor and Evaluate (ME)

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and providing governance. It typically addresses the following management questions:

- Is IT's performance measured to detect problems before it is too late?
- Does management ensure that internal controls are effective and efficient?
- Can IT performance be linked back to business goals?
- Are risk, control, compliance and performance measured and reported?

Domain 4. Monitor and Evaluate (ME)

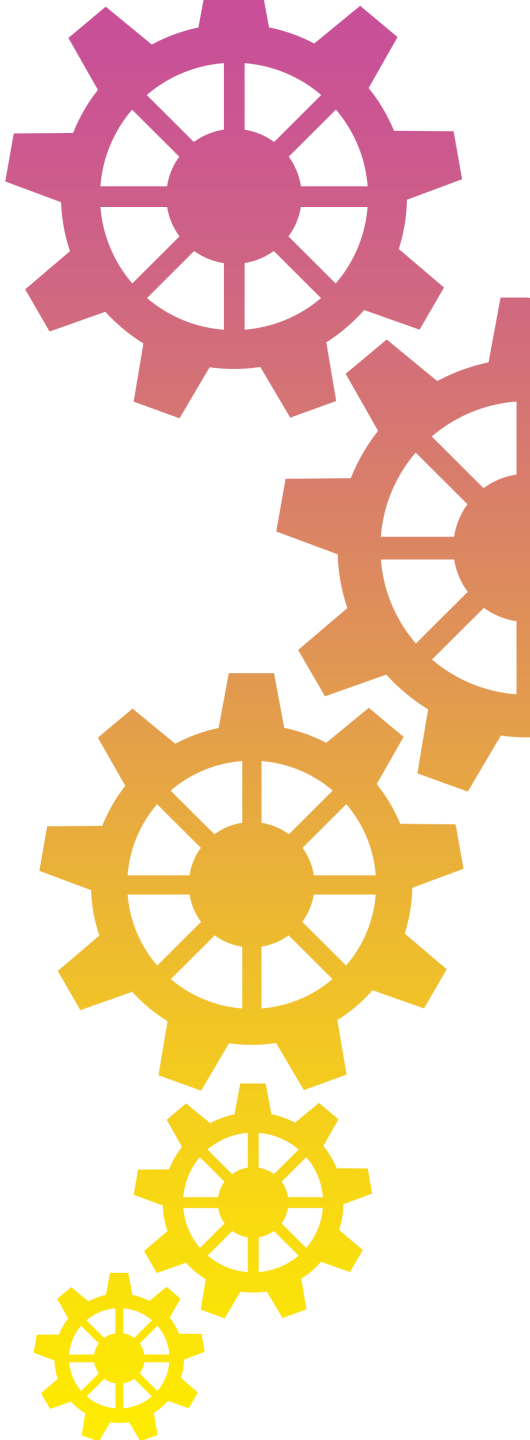
ME1 Monitor and Evaluate IT Performance

ME2 Monitor and Evaluate Internal Control

ME3 Ensure Regulatory Compliance

ME4 Provide IT Governance

Business Continuity Management



What is Business Continuity Management?

Business continuity management (BCM) prepares organizations for future incidents or crises that could interfere with the achievement of business objectives. Crisis management (CM) is a key component of BCM and deals with communicating pertinent information about the crisis to the organization's stakeholders.

All organizations will eventually face business interruptions. A well-defined BCM/CM plan is like an insurance policy for the organization — it helps to ensure that the organization will continue to be viable and meet stakeholder expectations.

Internal audit's breadth and depth of skills and qualifications, position in the organization, and in-depth knowledge of organization-wide operations position it well to make meaningful contributions to the development, implementation, and assessment of an organization's BCM and CM initiatives.

Key Components of Business Continuity Management

BCM is a risk management approach based on business value. It aligns business continuity capabilities with risks.

The goal of BCM is to enable any organization to restore critical operational activities, manage communications, and minimize financial and other effects of a disaster, business disruption, or other major event.

Types of Interruptions

BCM seeks to manage internally and externally generated threats. Each threat can have varying degrees of impact on the organization's business processes, which could adversely affect regulatory compliance, personnel safety, protection of the environment, the ability to maintain operating standards and satisfy contractual requirements, and the organization's brand/reputation.

Types of Interruptions

Types of interruptions include:

- Cyberattack
- Disease/pandemic
- Earthquake/tsunami
- Fire
- Flood
- Hurricane/tornado
- Labor disruption
- Production failure/outage
- Product contamination
- Sabotage
- Service or product outage for key business partners/vendors
- System failure
- Terrorism
- Utility outage

Role of Internal Audit in Business Continuity Management

Internal audit's roles may involve assurance and advisory services before, during, and after a crisis.

Assurance engagements may be performed to verify that BCM and CM are effective.

Advisory services may be performed to help management focus on planning activities and coordinate BCM and CM with risks and controls.

During a crisis, internal auditors also may be expected and authorized to perform critical non-auditing roles to serve the needs of the organization.

Internal Audit Activities Before a Crisis

Internal audit's evaluation of BCM, and specifically the CM plan, may help ensure that the CM plan remains relevant to organizational priorities in the event of a crisis.

Following are typical activities in which internal audit may be engaged before a crisis:

- Share knowledge of leading developments for BCM with executive management and the audit committee.
- Specifically consider BCM as a risk facing the organization and consider residual risks in the development of the annual audit plan.

Internal Audit Activities Before a Crisis

- Evaluate key business partner arrangements for appropriate contractual terms, including service-level agreements, right-to-audit clauses, and requisite reporting to management regarding the partner's control environment.
- Advise management in its performance of BCM risk assessments or evaluate the accuracy of management's BCM risk self-assessments.
- Perform assurance engagements related to the BCP and/or CM plan, as part of the annual audit plan. Assurance engagements may include evaluation of plan components, communication protocols within the plan, and the operational aspects of the plan.
- If not established by the provisions of the internal audit charter or directives from the board, clarify and establish BCM roles for internal audit.

Internal Audit Activities During and After a Crisis

During the Crisis:

- Monitor and assess the organization's response to an event and be an active participant on the crisis management team.
- Monitor outage details for subsequent audits.
- Serve on a crisis management committee to ensure that risks associated with a crisis are understood and provide recommendations on alternate courses of action to management, as appropriate.
- Participate in the wider crisis management and recovery process for the organization, as agreed upon and authorized.

Internal Audit Activities During and After a Crisis

After the Crisis:

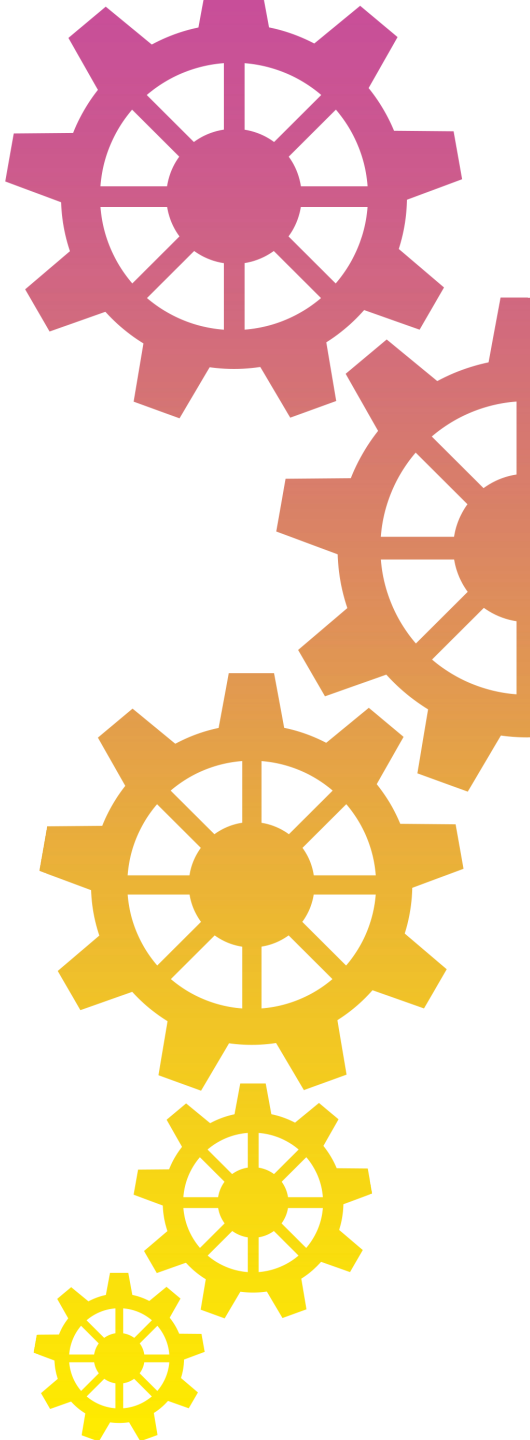
» Evaluate and report on the effectiveness of the organization's recovery efforts.

» Continue to assess risk, provide guidance, and help develop business improvement efforts.

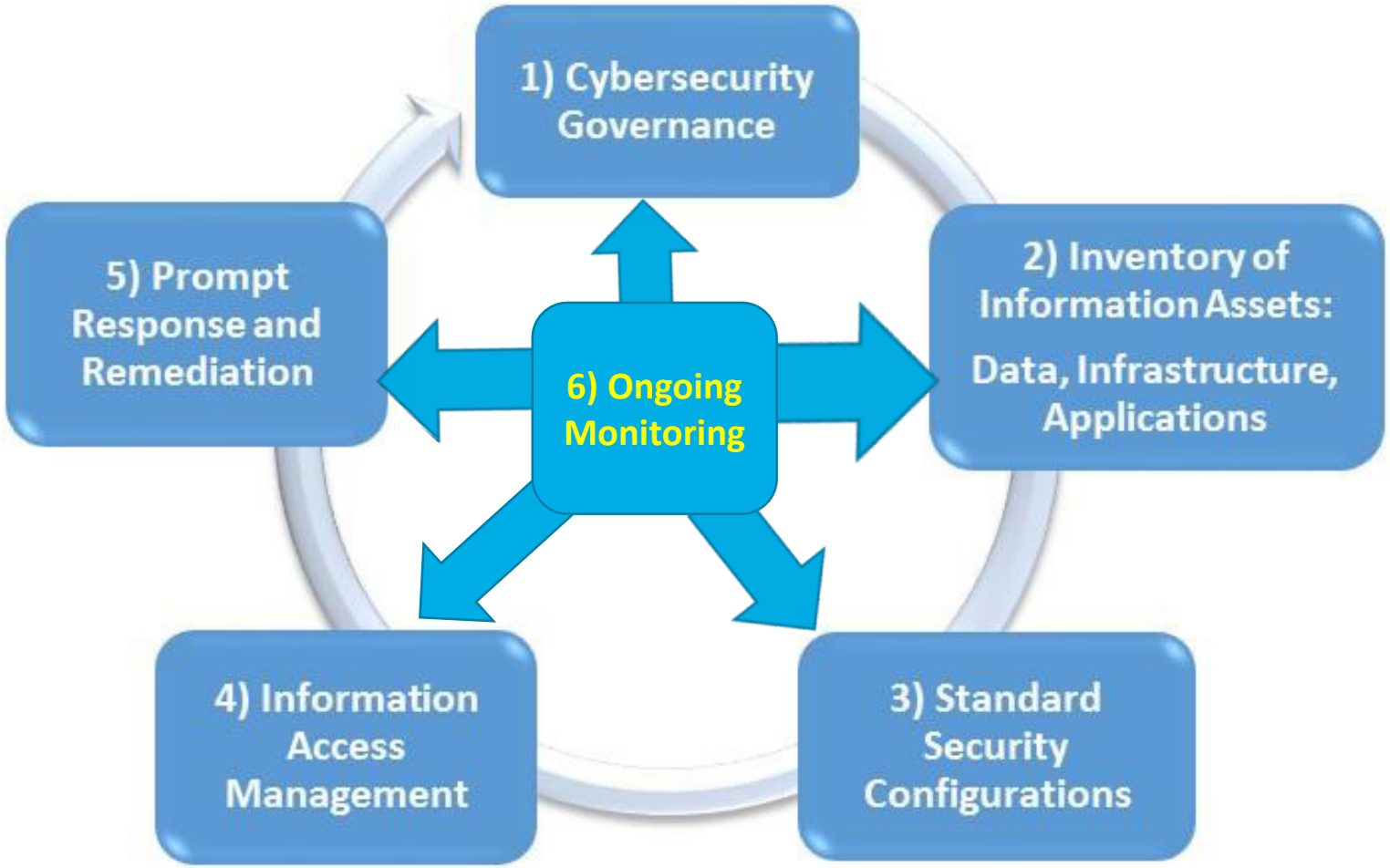
» Perform post-crisis reviews to identify opportunities for BCM activities and, specifically, for CM plan evolution.

» Perform assurance engagements to evaluate whether management performed and appropriately considered the results of root-cause analysis to update the BCP and CM plan, as needed. Participate in the organization-wide recovery process, as agreed upon and authorized per the BCP and CM plan.

Cyber Security



Cybersecurity Risk Assessment Framework



Cybersecurity Risk Assessment Framework

The six interdependent components of the framework illustrated above can be used to assess the design and operating effectiveness of management's cybersecurity controls and governance. Since deficiencies in any of the components will impact the overall effectiveness of cybersecurity, assessing how each is designed and operating with the others gives internal audit a basis for determining how well prepared the organization is to address cybersecurity risks. When components are not designed or operating well together, the organization is ill prepared to address cyber threats and emerging risks.

Component 1: Cybersecurity Governance

Strong cybersecurity governance depends on:

- ☐ Collaborating and collecting cybersecurity risk intelligence and expertise based on threats that could affect the organization.
- ☐ Setting risk appetite and tolerance.
- ☐ Planning for business continuity and disaster recovery in the event of an interruption.
- ☐ Responding promptly to security breaches.
- ☐ Establishing a culture of awareness of cybersecurity risks and threats.

Component 2: Inventory of Information Assets

When evaluating the organization's information assets, the following should be considered:

- Data
  - » Types (e.g., transactional, IT configuration, unstructured)
  - » Classification (enables standardization and prioritization)
  - » Environments (e.g., data warehouses, key data bases)
- Infrastructure repository of technology assets
  - » Servers
  - » Network devices
  - » Storage
  - » End-user devices (e.g., laptops, mobile devices)
- Applications
- External relationships
  - » Third-party hosted environments
  - » Sharing of data files with external organizations (e.g., vendors, regulatory bodies, governments)

Component 3: Standard Security Configurations

Centralized, automated configuration management software can be used to establish and maintain baselines for devices, operating systems, and application software. Using management software is more effective than managing systems manually or in a nonstandard fashion.

Component 4: Information Access Management

Management should consider implementing preventive controls such as having a process to approve and grant access to users based on job roles. Additionally, a process to detect when employees move within the organization would help to ensure that user access is adjusted and relevant to the new role.

Privileged administrative access is especially important. Users with the capability to access and release information are most susceptible to cybersecurity risk.

Component 5: Prompt Response and Remediation

The capability of the organization to promptly communicate and remediate risks indicates the program's effectiveness and level of maturity. Mature programs are able to continuously shorten the time to management response. One role of the second line of defense is to:

- ☐ Communicate risks that matter.
- ☐ Enact remediation.
- ☐ Track identified issues to resolution.
- ☐ Trend and report on resolution across the entity.

Component 6: Ongoing Monitoring

As a final component of this framework, continuous auditing of each of the five components described above when conducted will help to determine how risk is managed and how well corrective action is operating. The second line of defense is expected to implement a monitoring strategy designed to generate behavioral change that includes:

» Access-level evaluation and scanning that involves monitoring people with access to sensitive information to measure related cybersecurity risk.

» Vulnerability assessment: Regularly scanning systems is critical to identify vulnerabilities within the environment.

» Externally facing systems often pose the highest risks to organizations and should receive priority.

Component 6: Ongoing Monitoring

- Third-party risk assessments and monitoring: Programs can assist in assessing third-party vendors' risks and the level of security risk posed to the organization based on the services provided.
- Penetration testing: The second line of defense may conduct penetration testing for known vulnerabilities to assess preventive technical controls, as well as management's ability to detect and respond to attacks.
- Malware: Because vulnerabilities may be discovered after a device or software product was shipped to a customer, a process should be considered to regularly scan devices and products, identify vulnerabilities, and patch systems in order of priority (e.g., critical assets with critical patches first).
- Incident monitoring and response: This combination of processes allows an organization to detect, respond to, remediate, recover, and report to management in the event of a breach.

Role of the Internal Audit in Cyber Risk Assurance

As the risk landscape evolves and use of cloud services, mobile devices, and social media increase, cyber threats increase. Routinely, internal audit should discuss the organization's risk appetite with senior management and the board. Internal audit should also meet regularly with the organization's risk management leaders or committee to prioritize cybersecurity risks and threats to ensure resources are allocated to the most significant ones. Thus, it is essential for management to identify and develop a strategy to address the information systems and data assets most crucial to the organization and for internal audit to validate this with senior management and the board.

Role of the Internal Audit in Cyber Risk Assurance

The board and senior management look to internal audit for assurance on risk management and controls, including the overall effectiveness of the activities performed by the first and second lines of defense in managing and mitigating cybersecurity risks and threats.

The board needs to understand the information systems and data assets that are most crucial to their organization and gain assurance from the CIO, CISO, CSO, CTO, and CAE that controls are in place to prevent, detect, and mitigate cyber risks within the acceptable level of tolerance.

Role of the Internal Audit in Cyber Risk Assurance

Internal audit should ensure that board members are well-informed on common and industry-specific cyber threats and the impact that cybersecurity incidents may have on the organization.

The board and senior management may benefit from participating in awareness training and education sessions to gain an understanding of the organization's cyber threat profile.

The board will also be looking to internal audit to provide assurance that management has a strategy and plan in place to notify the board, enforcement authorities, customers, and the public in the event of a major breach.