IIA Malaysia e-techline
June 2022 Issue 3/22

STANDARDS AND GUIDANCE

AUDITING CYBER INCIDENT RESPONSE AND RECOVERY (BY IIA GLOBAL)

Cybersecurity attacks are increasing as the tools for detecting and exploiting vulnerabilities in networked systems and devices become increasingly sophisticated and commoditised. Nearly all organisations have some degree of risk exposure, and the potential impacts include a breach of customer data, direct financial loss, and physical manipulation of resources. Even with a defence-in-depth strategy, sometimes a flaw in design, implementation, or human nature can be exploited.

Controls are needed so that when a cyberattack is confirmed and an incident declared, an optimal response and recovery are ensured. Significant controls can be grouped into the following high-level business objectives:

- **Incident Response Planning**

  Policies and procedures should be established to guide the determination of whether an incident has occurred and what to do about it. The planning should involve key stakeholders, define roles and responsibilities, and be tested as appropriate to promote awareness and execution.

  Documenting and applying the lesson learned from cyber incidents can help an organisation improve its protective defences, detection of cyber incidents, and resilience.

- **Incident Identification**

  Processes to analyse data from detective controls lead to the determination of the existence of a cyber incident, which typically is the trigger for the execution of one or more response plans.
  When a decision is made to declare a cyber incident, the appropriate response and recovery plans need to be invoked.

- **Communications**

  There are many potential stakeholders in cyber incidents, so each response plan should incorporate a communication strategy for appropriate and timely notification of impacts and resolution efforts.

  Ideally, key stakeholders would be notified timely that a response plan has been invoked, and they would have previously practiced or at least reviewed and understood on their respective roles.

  Reporting cyber incidents as well as remediation efforts to external bodies, such as law enforcement or regulatory agencies, may be required in some cases.

- **Technical Response and Recovery**

  The nature of the incident largely determines the necessary technical remediation and restoration controls, often involving coordination of efforts internally and externally.

  Cyber incident response and recovery processes require sufficient and adequately trained resources to execute the plans and react effectively to rapidly unfolding threats.

  Specialised training, interaction with cyber defence organisations, and periodic testing of incident response and recovery controls can provide the technical skills necessary to mitigate the risks of cyberattacks.

What should Internal Auditors do?

IPPF *Standard* 1210 - Proficiency specifically identifies internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

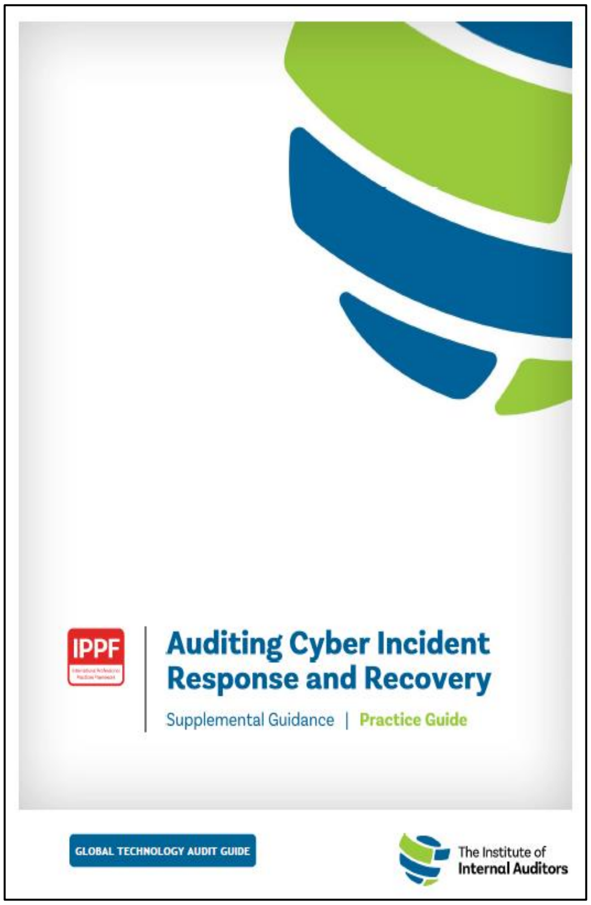
Stakeholders rely on independent, objective, and competent assurance services to verify whether cyber incident response and recovery controls are well-designed and effectively and efficiently implemented.

IPPF *Standard* 2000 – Managing the Internal Audit Activity stated that the chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organisation.

The internal audit activity adds value to the organisation when it provides such services in conformance with the *Standards* and with references to widely accepted control frameworks, particularly those expressly used by the organisation information technology and information security functions.

The internal audit activity – the third line – provides independent assurance services and consulting services regarding the adequacy and effectiveness of IT-IS processes, including cyber incident response and recovery controls. The internal audit activity should consider cyber incident response and recovery risks in its planning and proritisation of its audit engagements.

By working closely with IT and IS, the internal audit activity can ensure senior management and the board can get a clear and comprehensive view of the organisation's preparedness for cyber incidents.



IPPF

Auditing Cyber Incident Response and Recovery

Supplemental Guidance | Practice Guide

GLOBAL TECHNOLOGY AUDIT GUIDE

The Institute of Internal Auditors

Reference:
https://www.theiia.org/en/content/guidance/recommended/supplemental/gtags/gtag-auditing-cyber-incident-response-and-recovery/

STANDARDS AND GUIDANCE

INTERNAL AUDIT AND FRAUD (BY IIA GLOBAL)

Fraud risks may be internal or external to the organisation and include collusion, under- or over-reporting, misappropriation of assets or data, misrepresentation, falsification of documents, and destruction of records.

The internal audit activity contributes to fraud deterrence by providing assurance on the adequacy and effectiveness of fraud risk governance and management and advising on opportunities for improvement.

The IIA's position paper, The Three Lines Model, emphasises the importance of clear and consistent tone from the top, collaboration across the organisation, and the independence of the internal audit activity.

- **Board Roles**

  The board has ultimate responsibility for effective fraud risk governance and helps set the appropriate tone at the top. The board may appoint one of its members or an executive leader to champion fraud risk awareness and help coordinate activities.

  A board may establish a separate audit committee to oversee the internal audit activity and to assist in the monitoring and oversight of fraud risk, including controls to prevent or detect fraud by management.

- **Management Roles**

  Management is charged by the board with achieving the objectives of the organisation and has the primary responsibility for monitoring and controlling processes to prevent, deter, detect, and recover from fraud.

- **Management: First Line Roles**

  In their day-to-day activities, those with first line roles are expected to implement and monitor fraud risk and controls. They may also be responsible for helping design the policies, procedures, and tools for fraud risk assessment, analysis, controls, and monitoring, including the use of data analytics to prevent and detect fraud.

- **Management: Second Line Roles**

  Where separate specialist second line functions are established, they generally lead fraud risk management activities while working closely with senior management.

  Smaller organisations with limited resources may choose to co-source or outsource fraud risk expertise or rely on internal audit to take a more active role in fraud risk management activities.

- **Internal Audit: Third Line Roles**

  The internal audit activity provides assurance to the board and senior management on how effectively the organisation assesses and manages its fraud risks. This would include consideration of the overall coherence of fraud risk management activities and their alignment with organisational strategy and operations.

  Specific roles may include contributing to policy development and fraud training and supporting investigations. However, the internal audit activity's role in the governance and management of fraud risks should be clearly stated in its charter and reflected in its policies and procedures.

  This is to ensure senior management and the board understand and agree to the role and recognise any safeguards to help maintain independence of the internal audit activity and objectivity of internal auditors.

What should Internal Auditors do?

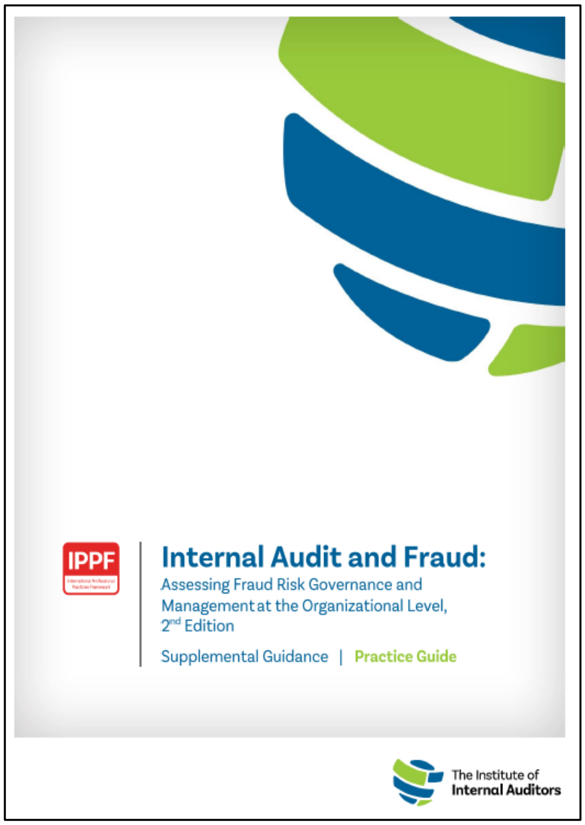
IPPF *Standard* 2120 – Risk Management stated that the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

IPPF *Standard* 2120.A2 further explained that the internal audit activity must evaluate the potential for the occurrence of fraud and how the organisation manages fraud risk.

The internal auditors should increase their awareness and understanding of organisational fraud risk governance and management.

This includes the role the internal audit activity can play and provide guidance on how to perform a fraud risk assessment at an organisational level.

Furthermore, internal auditors are required to consider the risk of fraud in their work.



IPPF

Internal Audit and Fraud:
Assessing Fraud Risk Governance and Management at the Organizational Level, 2nd Edition

Supplemental Guidance | Practice Guide

The Institute of Internal Auditors

Reference:
https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/practice-guide-internal-audit-and-fraud-2nd-edition/

STANDARDS AND GUIDANCE

AUDITING CYBERSECURITY OPERATIONS: PREVENTION AND DETECTION (BY IIA GLOBAL)

Cybersecurity refers to the technologies and processes designed to protect an organisation's information resources — computers, network devices, software programs, and data — from unauthorised access, disruption, or destruction.

According to The IIA's Three Lines Model, the IT and IS teams primarily responsible for information technology governance, risk management, and internal controls perform first and second line duties because they design and implement operational and oversight controls.

This guide references four external IT-IS control frameworks of standards, guidance, and best practices, which are:

- COBIT 2019 Framework: Governance and Management Objectives from ISACA.
- NIST Special Publication (SP) 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations from the National Institute of Standards and Technology (also referred to as NIST SP 800-53r5).
- NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (also referred to as the NIST Cybersecurity Framework [or NIST CSF]).
- CIS Controls Version 8 from the Center for Internet Security.

Coordination and collaboration between IT, IS, and the internal audit activity can provide the organisation's governing body and management with a comprehensive, tailored view of the effectiveness and efficiency of cybersecurity operations controls, including residual risks that may require further mitigation.

Security in Design

A systematic approach to analysing an organisation's cybersecurity operations controls in these groups may include a review of the IS team's involvement in the following areas:

Governance and risk management

The establishment and management of IT-IS policies and budgets, and processes ensuring alignment among organisational and IT-IS strategies. It includes an organisationwide approach to risks and related responses, with an emphasis on the internal controls designed and implemented to reduce the likelihood and impact of cyberattacks.

Technical planning and secure systems development

Processes to identify, procure, build, test, and authorise sufficient technologies and practices to deliver services to various user groups while ensuring control objectives are met.

Logical and physical access controls

Ensuring that the usage of information resources is limited according to the least privilege principle. For cybersecurity operations, the focus is typically on identity and authentication management tools and processes. However, another common objective is to ensure physical control of information resources is limited according to authorised business rules.

Prevention

The process for preventing cyberattacks employ technologies such as encryption, antivirus and data loss prevention software, and email and network filters that can thwart attempts to access or disrupt information resources or communications. Cybersecurity awareness training can help personnel avoid risks, such as phishing emails or other social engineering tactics.

- **Detection**

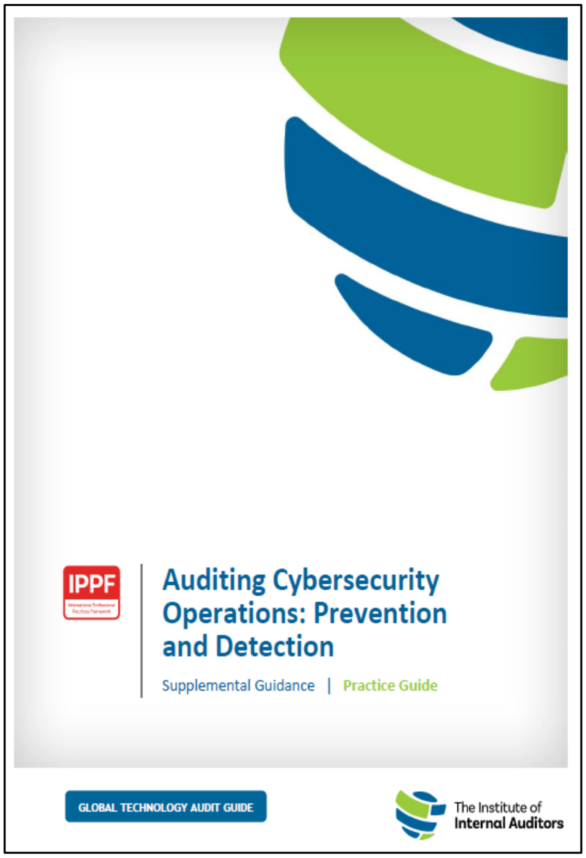
  When cyber incidents occur, management needs to be able to detect and analyse the attack's impact before beginning a process of response and recovery.

  IS team should examine the root causes of specific IT incidents to look for the common attributes of possible cyber incidents. The cybersecurity monitoring tools might even use artificial intelligence or machine learning technologies to assist in detecting cyber incident patterns.

What should Internal Auditors do?

IPPF *Standard* 2210.A1 – Engagement Objectives mentioned that internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

Auditing cybersecurity operations involves an engagement-level risk assessment, a specified scope and engagement objectives, and tests to evaluate the design and implementation of relevant controls to determine whether any significant risk exposures exist. The internal audit activity should consider cybersecurity risks in planning and prioritising its audit engagements.



IPPF

Auditing Cybersecurity Operations: Prevention and Detection

Supplemental Guidance | Practice Guide

GLOBAL TECHNOLOGY AUDIT GUIDE

The Institute of Internal Auditors

Reference:
https://www.theiia.org/en/content/guidance/recommended/supplemental/gtags/gtag-auditing-cybersecurity-operations-prevention-and-detection/

INTERNAL AUDIT FOUNDATION

INTERNAL AUDIT'S INVALUABLE ROLE IN CREATING A SENSE OF BELONGING AT WORK (BY DELOITTE, INTERNAL ADUIT FOUNDAITON AND IIA GLOBAL)

- **Bolstering Business Performance**

  Cultivating a diverse, equitable, and inclusive culture enables organisations to create a sense of belonging, which motivates people to bring the best of themselves to the job. Creating a sense of belonging for employees of diverse backgrounds is not only the right thing to do, but it is also an essential component of business performance. Lack of diversity, inequity, and exclusion are problems that demand a cultural shift.

- **Adding Distinct Value**

  As the connections between Diversity, Equity, and Inclusion ("DEI") and business performance expand, so too do the opportunities for internal audit to add value. Internal audit is attuned to pending disclosure requirements for environmental, social, and governance criteria, of which DEI is an important part.

- **Considering Program Risks**

  DEI programs often fail due to several common pitfalls including leadership constraints, incomplete talent data, and mistaking analysis for action. With its enterprise-wide view, internal audit is uniquely suited to help organisations identify and mitigate common risks to their DEI programs. Here are some risks for internal auditors to consider when performing a DEI review.

  - Using an incomplete methodology.
  - Focus too narrowly.
  - Relying solely on a top-down approach.
  - Seeking a quick fix.

What should Internal Auditors do?

IPPF *Standard* 1210 - Proficiency specifically identifies internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Internal audit offers an objective and independent vantage point from which to evaluate culture. It also has the methodologies and the base internal audit skill sets needed to consider DEI program risks and to create effective remediation plans. In other words, many of the skills required to assess the success of DEI initiatives are core skills of internal auditors.

Internal audit has an opportunity and an obligation to accelerate this movement toward greater diversity, equity, and inclusivity throughout the organisation, from top to bottom, by embedding DEI concepts into its
responsibilities and the services provide within its own functions. Internal audit can do its part in helping management meet its DEI objectives and shape corporate culture by enhancing the following roles and responsibilities with respect to DEI.

Deloitte. Internal Audit FOUNDATION The Institute of Internal Auditors

Diversity, Equity, and Inclusion (DEI) 101:

Internal Audit's Invaluable Role in Creating a Sense of Belonging at Work

Reference*:*
https://www.theiia.org/en/internal-audit-foundation/latest-research-and-products/

CHAMBERS ON INTERNAL AUDIT

5 STRATEGIES FOR MORE TIMELY INTERNAL AUDIT REPORTS (BY RICHARD CHAMBERS)

"The most brilliant of analyses and the most productive of audit findings seem to be forgotten during the trauma of report writing." – Lawrence Sawyer.

There are at least five strategies that (if deployed effectively) can substantially reduce the amount of time it takes to report audit results:

- **Share Internal Audit Results with Client "as you go"**
  Client "push-back" against an audit report can be intensified by the shock effect of seeing all of the results at once. Providing the client with results incrementally can help. Once the internal audit team gets to the point in the engagement where they are satisfied there is a reportable condition, you should share the information with your client, either informally or through an interim audit memorandum. Regular communication with clients during the audit, including sharing draft findings and recommendations in writing goes a long way toward fostering a positive reaction when the full report is presented for comment.

- **Eliminate or Reduce Levels of Review**
  Multiple levels of review within the internal audit department are often a major source of delays in audit reporting. Streamlining the review process and reducing the number of reviewers can shorten and speed up the process. Such tactics entail some risk as every additional review provides a fresh viewpoint and a different level or type of expertise, while having more-senior staff do reviews ensures more experienced eyes will examine the drafts. Sacrificing those could affect reports' accuracy, clarity, and constructiveness.

- **Use Team Editing or Report Conferencing**

  Bringing the audit team together with all of those who will edit or review the draft report for a single editing session can reduce reports' cycle time dramatically.

  This approach allows the internal audit team and the department's upper-level supervisors to discuss the draft report and propose changes without the endless back and forth of the usual editing process.

  Everyone sits around a table in a conference room, with the audit report projected onto a screen at the front of the room, and each person commits to not leaving that room until the review process is complete

- **Use Automated Working Papers' Report-Writing Features**

  Commercially available audit management systems often include features in which extracts from the electronic working papers are automatically imported into a draft report template. In such cases, the draft audit report virtually writes itself. This can generate major efficiencies in the report-writing process.

- **Streamline the Report Format**

  Internal audit departments that have successfully reduced their reports' cycle time generally produce leaner audit reports, which makes them not only easy to edit but easy to read. The shorter a report is, the less time it typically takes to write and edit.

  Complexity can also slow the review process and reaching consensus with clients can become onerous with longer reports.

  It is always tempting to include more detail in an internal audit report than the minimum needed to make the point, but the advice to new auditors is to tell the story clearly and succinctly.

What should Internal Auditors do?

IPPF *Standard* 2420 – Quality of Communications mentioned that communications must be accurate, objective, clear, concise, constructive, complete, and timely.

There are no quick solutions or easy answers to the age-old challenge of audit report timeliness. Internal audit departments that recognise they have a timeliness challenge and seek to reduce cycle time can make an impact.

Internal auditors need to pay great attention detail when drafting communications and consider the characteristics of quality communications outlined in the Interpretation of *Standard* because high-quality engagement communications are critical.

Internal auditors should also understand the organisation's expectations for communication, including stakeholder expectations regarding communication deadlines.

Reference*:*
https://www.richardchambers.com/5-strategies-for-more-timely-internal-audit-reports/

If you missed out the previous issues of e-techline, you may visit our website at https://iiam.com.my/technical-qa-services/e-techline/.