IIA Malaysia e-techline

February 2023 Issue 1/23

STANDARDS AND GUIDANCE

GTAG: AUDITING NETWORK AND COMMUNICATIONS MANAGEMENT (BY IIA GLOBAL)

Network and Communications Control Groups

Governance, Risk Management, and Administration

Governance and Risk Management

Governance pertains to the board’s processes for representing the stakeholders’ interests, which includes directing and authorising certain strategies and priorities.

Entity-level strategies and objectives for network and communications management may include compliance with applicable regulations and control frameworks, as well as decisions to outsource network infrastructure or otherwise engage critical service partners.

Administration

Network and communications services consist of processes, tools, and personnel working together to achieve multiple high-level objectives determined by governance and risk management processes.

Technical planning controls typically produce an overall design, or architecture, for the data network, as well as baseline configurations to guide the installation of approved technologies. Such controls also produce a timeline, often referred to as a roadmap, for the introduction and retiring of relevant technologies used throughout the organisation.

Zero trust principles emphasise granular identity verification and authentication controls. Deciding how and where to implement those principles to manage confidentiality and integrity risks is a significant concern for network and communications technical planning.

Domain Management

To manage data traffic between the organisation’s network and external systems, including the communications transport networks, a border gateway protocol (BGP) language has become a global standard.

Network Design

To help manage the complexity of an organisation’s data network, enterprise architects designate segments of the network – a set of IP addresses – to support specified groups of resources. The designations are usually determined by a combination of organisational data classification policies and each resource’s function and security categorisation.

Microsegmentation facilitates a zero-trust approach by decreasing the number of addresses in each segment, which helps increase the granularity of access controls. Data loss prevention and privacy-related controls are also facilitated by security zones.

Network Device Administration

Devices that act as intermediaries between the organisation’s computing and communications capabilities include hardware and related software applications. These devices are programmed to facilitate communications according to engineering best practices and internal business rules.

A review of network device administration controls would typically determine the strength of controls to achieve the following objectives:

- Network management hardware and software are properly installed and connected to monitoring systems, in accordance with internal requirements.

- Security event logs are programmed to capture an audit trail for significant actions, such as creating new administrator accounts or modifying any configuration items.
- Baseline configurations are managed to optimise controls for network performance and security.
- Changes to network and communications technologies or configurations, including security patches for relevant applications, are effectively implemented.
- Access to technology resources, both physical and logical, is sufficiently secured, with system administrator accounts authorised according to the least privilege principle.

Communications Management

The processes to manage an organisation's communication needs cover end user communication and collaboration tools, as well as facility infrastructure connections to telecommunications service providers.

Managing the operating relationships with various service providers is a significant concern for this grouping of controls. Performance, cost, and resilience factors all contribute to management decisions on which communication and collaboration services to provide the organisation.

Boundary Defense

External Connections

When the organisation engages with vendors to obtain data or services, a connection between the two-enterprise network (often called an interconnection) is typically established.

When end users attempt to connect a device to the enterprise network via the internet, commonly referred to as remote access, network controls may verify the identities of the person and the device, and ensure that the connection is adequately secured.

Network Security

Network security controls can be more narrowly defined as designed to achieve the following business objectives:

- Security technologies are implemented to protect resources in accordance with their risk-based categorisation.
- Security event logs are configured to capture data about significant actions, with enough information to promote individual accountability.
- Network management personnel work with IS teams to test controls and remediate any significant vulnerabilities identified.

Network Operations

The performance and availability of the data and communications ecosystem needs to be monitored, with issues resolved effectively and efficiently.

Business resilience objectives for the data network ecosystem largely consist of ensuring redundant, failover, and emergency communication capabilities, as well as developing and testing contingency plans.

Monitoring and Operations Assistance

Some types of network traffic and system usage monitoring are performed by network security and IS teams; however, the monitoring usually associated with network operations contributes primarily to service availability, rather than security, objectives.

Nevertheless, some types of cyberattacks result in traffic anomalies or disruptions to network functions, including changing configuration settings. Therefore, network monitoring processes should be coordinated with security controls to identify potential cyber incidents in a timely manner.

... 2

- **Resilience**

  Network and communications management personnel are often prominently involved in resilience planning efforts, sometimes referred to as business continuity or disaster recovery planning. In some organisations, resilience program ownership may be delegated to a member of network management. Additionally, the network hardware, software, and communication services are critical infrastructure elements that typically have contingency plans, redundant or alternate paths, and geographic distribution capabilities to enhance their resilience.

What should Internal Auditors do?

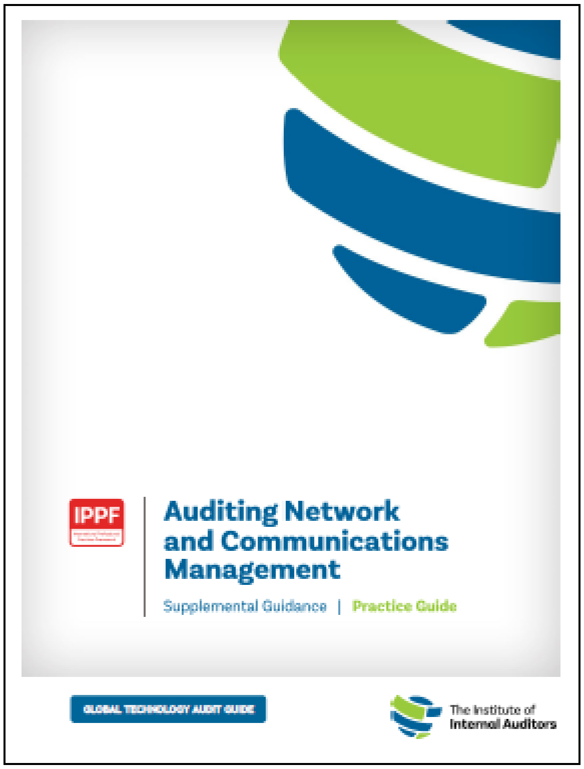
IPPF *Standard* 1210.A3 – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

IPPF *Standard* 2110.A2 – The internal audit activity must assess whether the information technology governance of the organization supports the organisation's strategies and objectives.

For internal auditors to provide valuable assurance and consulting services regarding the objectives, risks, and controls over network and communications management, it is necessary to understand the key processes and controls.

Network and communications management risks and controls can be conceptually organized according to the model of governance, risk management, and internal controls provided in the *Standards*.

This Guide helps internal auditors find the additional information needed to build tailored audit programmes and meaningful tests of control adequacy and effectiveness.



IPPF

Auditing Network and Communications Management

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-network-and-communications-management/

TONE AT THE TOP

THE DATA DILEMMA: EMPOWERING INTERNAL AUDIT'S USE OF TECHNOLOGY (BY IIA GLOBAL)

Knowledge is power, and in a modern business context that means leveraging technology for effective use of data in planning, strategising, and decision making. Unfortunately, organisations may not be benefiting from all the advantages that advanced technologies can offer to support their goals. When internal audit is outpaced by other parts of the organisation in embracing technology, the valuable assurance and advisory services it can provide may also be lagging.

Boards should be mindful of their internal audit function's relationship with technology, ensure sufficient resources to acquire needed technology, and push internal audit leaders to embrace data analytic.

A Range of Benefits

- **Timely Metrics**

  Real-time information delivered by advanced technologies can put companies in a better position to track performance and quality and make necessary adjustments and remediation. Real-time indicators make it possible to better align internal audit goals with the company's strategic objectives as well as its main threats and opportunities. At the same time, the elimination of manual and repetitive tasks enhances productivity and frees internal audit professionals to provide higher-value insights.

- **Better use of Data**

  As organisations gather or gain access to more detail, automated analytics tools make it feasible to perform more comprehensive and focused reviews that are more likely to deliver useful insights for decision making. In addition, billing data can be mined to ensure that it jibes with contract terms.

- **Faster Risk Identification**

  It often requires poring over an enormous amount of data to identify anomalies that can indicate fraud, errors, or other issues to be addressed. Advanced technologies can automate such reviews to help highlight anomalies or other risk considerations, leaving internal audit better able to make data-based identifications of high-risk areas. In addition, when auditors can easily select high-risk samples, they spend less time testing and cause less disruption to audit clients.

- **Continuous Monitoring**

  A data-driven audit can define thresholds that will trigger alerts for fraud, tagging items by a certain number, amount, category, or frequency of transaction. Finding these cases can enable internal audit to identify potential breaches in authority, policy, or procedure on a proactive, automated basis.

- **Ease in Sharing Data**

  Once data has been gathered and analysed, readily available software tools make it possible to create dashboards and data visualisations that communicate results easily and effectively. Instead of columns of data or complicated charts, facts, and trends can be shown in digestible pieces. These graphics can also be tailored to each audience, providing a concise overview for the board or senior management, and allowing for a deeper dive into the business unit being audited. Stakeholders can also receive these reports more quickly than in the past.

Barriers to Overcome

- **Insufficient Investment**

  Although technologies such as data analytics and AI have received a great deal of attention, internal audit functions may not yet be able to make the best use of them.

- **The need to Upskill the Team**
  Proficiency in the use of data analytics goes beyond simply learning a new program. Instead, internal audit functions need team members who have the data science and IT skills to put data analytics to work. Team training and development are integral to making the best use of existing innovations and leveraging new ones.

What should Internal Auditors do?

IPPF *Standard* 1210 – Proficiency mentioned that the 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.

Technology can help internal audit teams balance resource constraints while still providing coverage over traditional high-risk areas.

Because of the large volume of data being produced, organisations may find themselves with a great deal of information but not necessarily as much knowledge. Given its holistic knowledge of the organisation, internal audit is well suited to use these tools to translate data into business insights.

Using advanced technologies in the internal audit function provides a wide range of benefits to the company. Internal audit teams can eliminate low-value activities and work smarter in their selection and accomplishment of audits, as well as deliver enhanced insights and assurance.

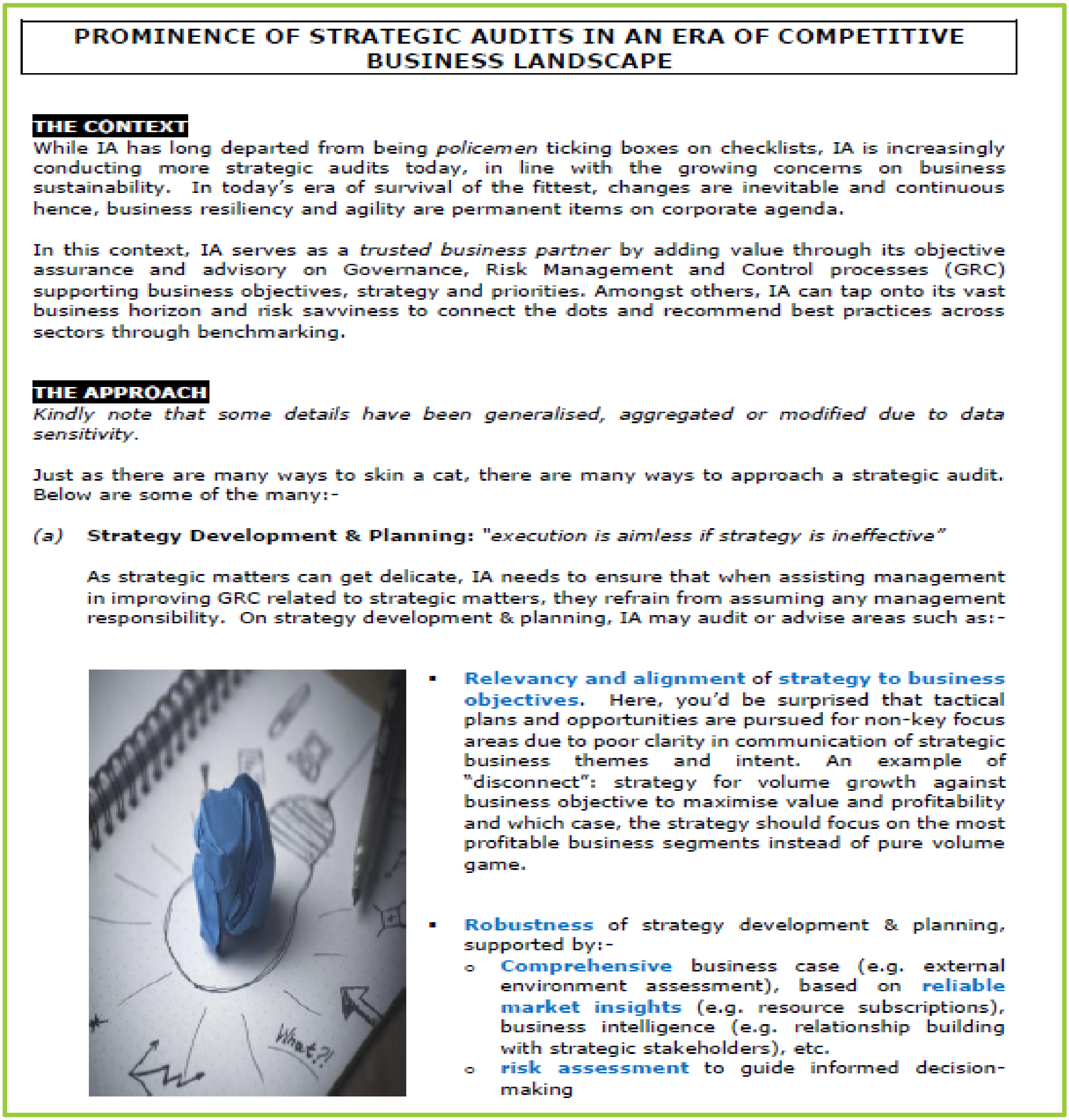
Reference:
https://www.theiia.org/en/content/articles/tone-at-the-top/2022/tone-at-the-top-dec2022/

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/.

Scan the QR Code below to complete an e-techline survey.

**NEW SECTION* - TECHNICAL WRITER*

PROMINENCE OF STRATEGIC AUDITS IN AN ERA OF COMPETITIVE BUSINESS LANDSCAPE (BY JAVEN KHOO AI WEE, CIA, CISA, CFE)



PROMINENCE OF STRATEGIC AUDITS IN AN ERA OF COMPETITIVE BUSINESS LANDSCAPE

THE CONTEXT

While IA has long departed from being *policemen* ticking boxes on checklists, IA is increasingly conducting more strategic audits today, in line with the growing concerns on business sustainability. In today's era of survival of the fittest, changes are inevitable and continuous hence, business resiliency and agility are permanent items on corporate agenda.

In this context, IA serves as a *trusted business partner* by adding value through its objective assurance and advisory on Governance, Risk Management and Control processes (GRC) supporting business objectives, strategy and priorities. Amongst others, IA can tap onto its vast business horizon and risk savviness to connect the dots and recommend best practices across sectors through benchmarking.

THE APPROACH

Kindly note that some details have been generalised, aggregated or modified due to data sensitivity.

Just as there are many ways to skin a cat, there are many ways to approach a strategic audit. Below are some of the many:-

(a) **Strategy Development & Planning:** "*execution is aimless if strategy is ineffective*"

As strategic matters can get delicate, IA needs to ensure that when assisting management in improving GRC related to strategic matters, they refrain from assuming any management responsibility. On strategy development & planning, IA may audit or advise areas such as:-

- **Relevancy and alignment** of **strategy to business objectives.** Here, you'd be surprised that tactical plans and opportunities are pursued for non-key focus areas due to poor clarity in communication of strategic business themes and intent. An example of "disconnect": strategy for volume growth against business objective to maximise value and profitability and which case, the strategy should focus on the most profitable business segments instead of pure volume game.
- **Robustness** of strategy development & planning, supported by:-
  - **Comprehensive** business case (e.g. external environment assessment), based on **reliable market insights** (e.g. resource subscriptions), business intelligence (e.g. relationship building with strategic stakeholders), etc.
  - **risk assessment** to guide informed decision-making

- **Balanced scorecard** and **employee performance metrics** are also evaluated to assess whether key performance indicators have been established and cascaded to align efforts and resources towards meeting corporate strategy.

- Also of interest to IA is on **people capability** to determine whether talents involved in strategic activities are **qualified** to do the job, by establishing whether:-
  - **training plan** is intact to address any capability gap.
  - **succession planning** is established for business critical positions which often include strategic positions.

(b) **Strategy Execution:** *"strategy is useless if execution is ineffective"*

In assessing both effectiveness and efficiency of strategy execution, the following areas are often evaluated by IA, amongst others:-

- **Compliance** with business opportunity **screening** and **sanction processes**, and **regulatory requirements** especially where the strategy encompasses different geographics with localised laws and regulations.

- **Comprehensiveness and timeliness** of **monitoring and reporting** to Management, including issues escalation for solutioning and way forward.

  Where **systems and/or tools** are utilised for **progress tracking**, IA often assesses the **discipline** inculcated amongst users to sufficiently leverage on the system as a **single source of truth** so that the reported status is consistent and accurate against actual status. If adequately utilised, the features and application functions in the systems could be used to **automate reporting** through dashboarding while minimising human errors.

- Since strategy execution involves multiple parties across the company and relevant external parties, **interfacing activities** are also evaluated for **seamless coordination** towards delivering Client's business agenda.

(c) **Post-Implementation Review:** *"execution success to be measured against intended results"*

- In order to safeguard Client's interest, **Return on Investment (ROI) monitoring** or **investment review** should be performed, monitored and reported periodically to allow for **timely intervention**, and facilitate effective portfolio review, e.g. divestment, consolidation.

- **Lessons learnt** should be captured not just upon completion of projects, but also for deals that did not pan out. Infact, lessons learnt on similar opportunities should be referred in order to **avoid repeating painful mistakes**, and commit to **continuous improvement** through sharing of best practices. **Knowledge Management** is especially important if the Client is newly set-up. With people come and go, such lessons learnt can provide a reference to new talents.

- Proper **record management** (creation, labelling, usage/sharing, storing, retention/disposal, etc.) is important since most documents related to strategy development, business plans, decision papers, economic models, trade secrets, etc. are **sensitive in nature**.

Client is often hostile when IA wants to audit their strategic activities. The impression is often of IA wanting to criticise their competency in managing business operations. This is never the case as IA's expertise and responsibility are in strengthening GRC or corporate governance which will assist and complement Client in meeting its strategic, operational, financial, and compliance objectives.

Strategic activites are often fluid and agile. Hence, IA aims to help simplify Client's processes to enable them to repond to market changes at pace.

IA does not measure its performance by the quantity of additional controls recommended to Client, or number of audit issues raised against Client. In short, both IA and Client strive to achieve mutual objectives and that is to add-value to the organisation as a whole, and IA helps Client to improve its business operations through objective appraisal of GRC.

In addition, IA is increasingly being leveraged on by Client to elevate business issues at Audit Committee (AC), especially items that have not been promptly and effectively resolved by Senior Management. This is a testimony that Client is seeing value in IA as a trusted business partner.

In order to add value to a strategic audit, IA has to demonstrate business acumen or ability to see the big picture and analyse the small details, understand all the functional areas of Client company and the interdependencies, etc. To do this effectively, IA ensures that it is sufficiently staffed both in capacity and capability, leverages on strategic tools such as Porter 5 Forces analysis, SWOT analysis, or resources such as Gartner in drawing such understanding of Client's business operations.

(word count: 1,000)

Penned by,
Javen Khoo Ai Wee, CIA, CISA, CFE
CMIIA Membership No. 211787