SNG
Grant Thornton

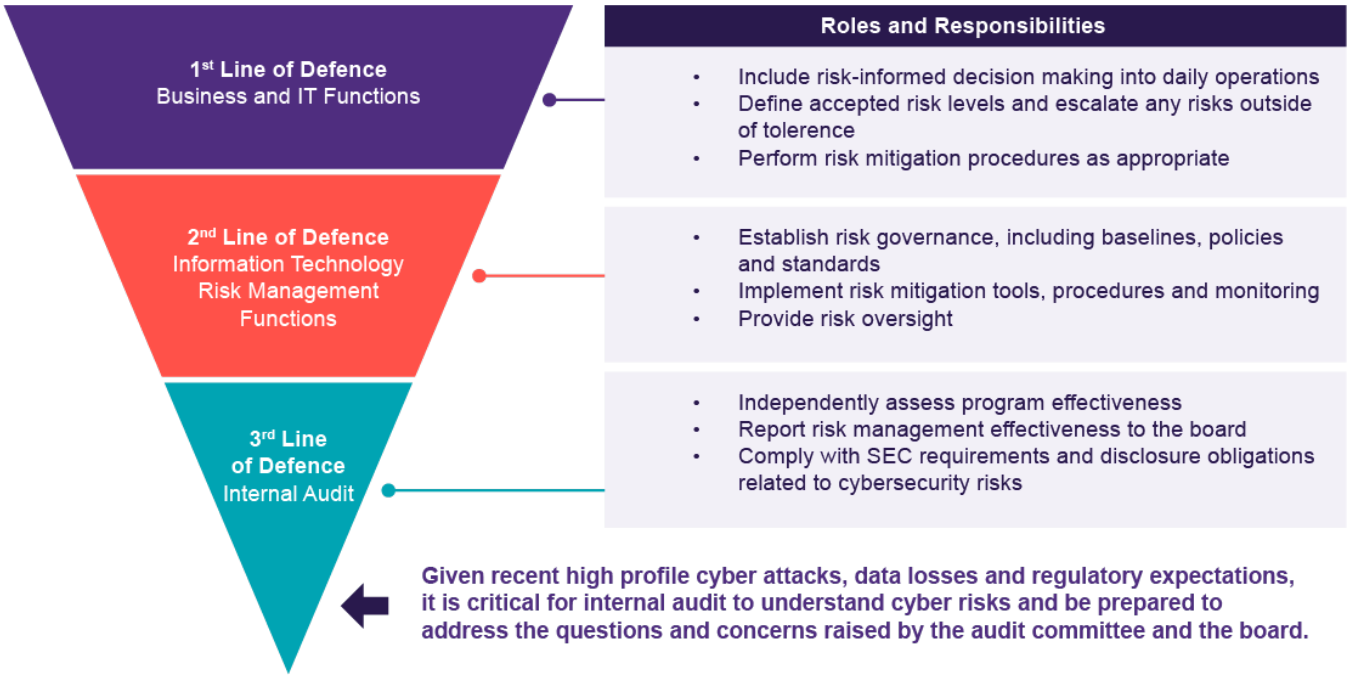
# Strengthening Cyber Security:

## The crucial role of Internal Audit

# The Role of Internal Audit in Enhancing Cybersecurity

In the ever-evolving landscape of cybersecurity threats, organisations face numerous challenges in safeguarding their digital assets and sensitive information. To navigate these challenges effectively, organisations can leverage the expertise of their internal audit functions.

Internal auditors serve as the third line of defence in cybersecurity governance, playing a crucial role in ensuring robust risk management practices and regulatory compliance. While the first line comprises of operational management responsible for day-to-day cybersecurity activities and the second line includes risk management and compliance functions, internal auditors provide independent assurance and evaluation of these processes.




Internal auditors play a crucial role in evaluating and enhancing cybersecurity measures, guided by established frameworks and standards.

### Assessing Cybersecurity Governance

Effective cybersecurity governance is essential for setting the tone at the top and ensuring that cybersecurity objectives align with the organisation's overall strategic goals. Internal auditors assess the establishment of cybersecurity policies, procedures, and frameworks, as well as the clarity of roles and responsibilities within the organisation. By evaluating the governance structure, internal audit functions help identify areas for improvement and ensure that cybersecurity efforts are integrated into the organisation's overall governance framework.

**Statistical Insights:**

1. **Cybersecurity Governance Impact**: According to a study by the International Data Corporation (IDC), organisations with strong cybersecurity governance frameworks, experience 30% fewer security incidents compared to those with inadequate governance structures.
2. **Internal Audit Contribution**: Research conducted by the Institute of Internal Auditors (IIA) reveals that 82% of organisations consider internal audit functions as being instrumental in assessing and improving cybersecurity governance.
3. **Organisational Integration**: A Grant Thornton Business Pulse report that surveys mid-market businesses showed that 45% of business implemented a cybersecurity framework and 37% have defined cyber strategies, policies and procedures. While only 29% have a dedicated or delegated team focusing on cybersecurity.

The statistics underscore the vital role of internal audit functions in reinforcing cybersecurity governance within organisations.

## Evaluating Risk Management Practices

Cybersecurity risk management involves identifying, analysing, and mitigating risks related to information technology and security. Internal auditors play a critical role in evaluating the organisation's risk management practices, including the identification of cyber risks, the effectiveness of risk assessment methodologies, and the adequacy of risk mitigation strategies. By conducting comprehensive risk assessments and evaluating risk management processes, internal audit functions help organisations prioritise their cybersecurity efforts and allocate resources effectively.

According to the IBM Security and Ponemon Institute's "Cost of a Data Breach Report 2023", the global average cost of a data breach increased by 2.3% compared to the previous year, reaching $4.45 million. The same report also highlights that the average time to identify and contain a data breach was 196 days, indicating the prolonged exposure of sensitive data and potential for extensive damage.

Data privacy has emerged as a significant risk for businesses, with the proliferation of data breaches posing substantial threats to both organisational reputation and financial stability. Various countries have responded to this challenge by implementing stringent data privacy laws and regulations. Internal audit functions are well-positioned to assess and mitigate this risk effectively.

## Enhancing Control Processes

Cybersecurity control processes are the frontline defenses against cyber threats. Internal auditors assess the design and effectiveness of cybersecurity controls, including technical controls, administrative controls, and physical controls. By evaluating control processes such as access controls, encryption mechanisms, and incident response procedures, internal audit functions help identify weaknesses and vulnerabilities in the organisation's cybersecurity defenses. Additionally, internal auditors ensure that control processes are properly implemented and monitored to detect and respond to cyber threats in a timely manner.

One area where companies often fall short is in cloud assurance. While major cloud service providers like Microsoft Azure (MS) and Amazon Web Services (AWS) offer robust security measures, the responsibility for configuring and securing the environment ultimately lies with the organisation. In the shared cloud model, where resources are shared among multiple users, ensuring the proper configuration and implementation of security measures becomes even more critical. Many companies mistakenly believe that once they migrate to the cloud, all security concerns are automatically addressed by the provider.

However, inadequately configured environments can leave organisations vulnerable to cyber threats. According to a recent survey by McAfee, 83% of organisations store sensitive data in the cloud, yet only 29% have implemented proper security measures to protect it. This highlights the urgent need for organisations to enhance their cloud security practices.

## Leveraging Cybersecurity Topical Requirements

The cybersecurity topical requirements published by the IIA serve as a valuable resource for internal audit functions. These requirements provide a structured approach to assessing cybersecurity practices, covering key areas such as governance, risk management, and control processes. By following these requirements, internal audit teams can ensure that their assessments are comprehensive and aligned with industry standards. Additionally, the use of cybersecurity topical requirements facilitates consistency and comparability across internal audit engagements, enabling organisations to benchmark their cybersecurity practices against industry peers.

## Conclusion

In conclusion, internal audit functions play a crucial role in enhancing cybersecurity within organisations. By leveraging established frameworks and standards, such as the cybersecurity topical requirements published by the IIA, internal auditors help organisations assess and improve their cybersecurity governance, risk management, and control processes. By conducting thorough assessments and providing valuable insights, internal audit functions contribute to strengthening the organisation's cyber posture and mitigating the risks associated with cyber threats.

# Contact Us

**Kudakwashe Charandura**
Cyber Advisory
kudakwashe.charandura@sng.gt.com

**Maria Pretorius**
Director and Head: BRS
maria.pretorius@sng.gt.com