ICPAK

Credibility . Professionalism . Accountability

CRITICAL CYBER SECURITY REQUIREMENTS FOR BOARDS AND AUDIT COMMITTEES

In Fulfilling Virtual Oversight Roles

TECHNOLOGY IN MODERN BUSINESS ENVIRONMENT

- ❑ Technology transcends part of every business activity and has become a strategic pillar to the businesses.
- ❑ The IT functions within organizations have evolved from being in the back seat to the front seat and from the front seat to the driver’s seat.
- ❑ Recent developments have demonstrated that information technology is now embedded deeply in the business functions and are required to drive transformational changes and has the potential to disrupt the existing business models even in mature industries

TECHNOLOGY IN MODERN BUSINESS ENVIRONMENT

“The world is shifting past the digital transformation era, to have a competitive advantage and ensure “survivability”. Most global businesses are now adopting data driven, smart and transformative technologies. Data is everything and is everywhere “

“Digital has become the need of the hour and the most effective enabler for creating a differential and unique competitive advantag “

TECHNOLOGY IN MODERN BUSINESS ENVIRONMENT

S Social	M Mobile	A Analytics	C Cloud
• Social Media engagement • Connected Customers • Collaboration • Communities • Crowd Sourcing	• Value through Micro Moments • Collaborative innovation on the Move • Customer Connect • All channel experience • Geo-Trageting	• Discovering Value through Patterns and Predictions • SEO • SEM	• Business Agility • Collaboration • Economies of Scale • Globalization • Competetivesness

TECHNOLOGY IN MODERN BUSINESS ENVIRONMENT

- ❑ The information technology which was once a cost centre has now become a strategic business imperative.
- ❑ Consequently, businesses are forced to evolve and enmesh the use of information technology to stay relevant, maintain competitiveness and pursue differentiation advantages
- ❑ **But the use of information technology also bring risks with it**,
- ❑ **Data breaches are a reality**: While 100% guarantee to prevent an organization from data breaches and cyber incidents is not possible, it is possible to adopt some basic principle based structural and governance changes in an organization and implement cyber hygiene to mitigate such risks.

IS IT POSSIBLE FOR AN ORGANIZATION TO PREVENT SECURITY INCIDENTS?

Credibility. Professionalism. Accountability

Is it possible for an organization to prevent security incidents?

ARE YOU ACCONTABLE?

If a data breach happens what is the accountability of the Board Members, CEO, CXO and other senior executives?

The board of directors should establish a strong risk management culture in the organization

CORE PRINCIPLES FOR BOARD OF DIRECTORS ON CYBER RISK

ICPAK

Credibility. Professionalism. Accountability

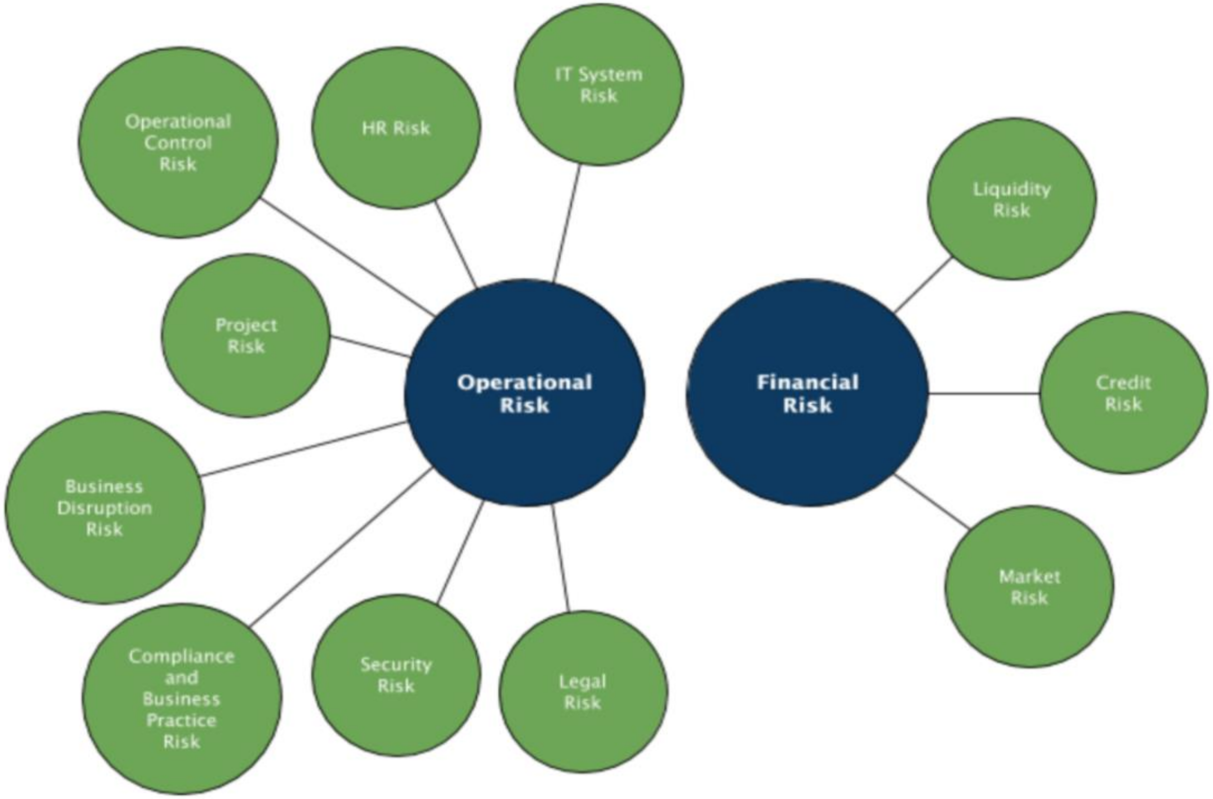
Fusion of National Association of Corporate Directors (NACD) with World Economic Forum - Cyber Risk Management Principles

P1:CYBER RISK EMBEDDED IN THE ENTERPRISEWIDE RISK MANAGEMENT

- ❑ While the overall risk assessment requires both qualitative and quantitative analysis, the investment in security could focus on ROSI (returns on security investment)
- ❑ An enterprisewide risk management framework should consider the following four pillars to incorporate the cyber-risk in the overall operational risk management scope:
  - ❑ Governance, Accountability and Ownership
  - ❑ Common Taxonomy, Cybersecurity Awareness and Security Policies
  - ❑ Skills and Competencies
  - ❑ Metrics, Reporting and Preparedness

P1:CYBER RISK EMBEDDED IN THE ENTERPRISEWIDE RISK MANAGEMENT

A holistic risk assessment that includes both financial as well as non-financial risks



P2: LEGAL IMPLICATIONS

- ❑ Board is ultimately held liable and responsible for large cyber incidents. This is because it is the leadership that sets the tone for the rest of the organization.

- ❑ Severe consequences of cyber attacks can expose organisation’s directors to legal Risks .
- ❑ More cyber-mature industries also have regulatory guidance and requirements when it comes to the cybersecurity responsibilities of the Board of Directors

P2: LEGAL IMPLICATIONS

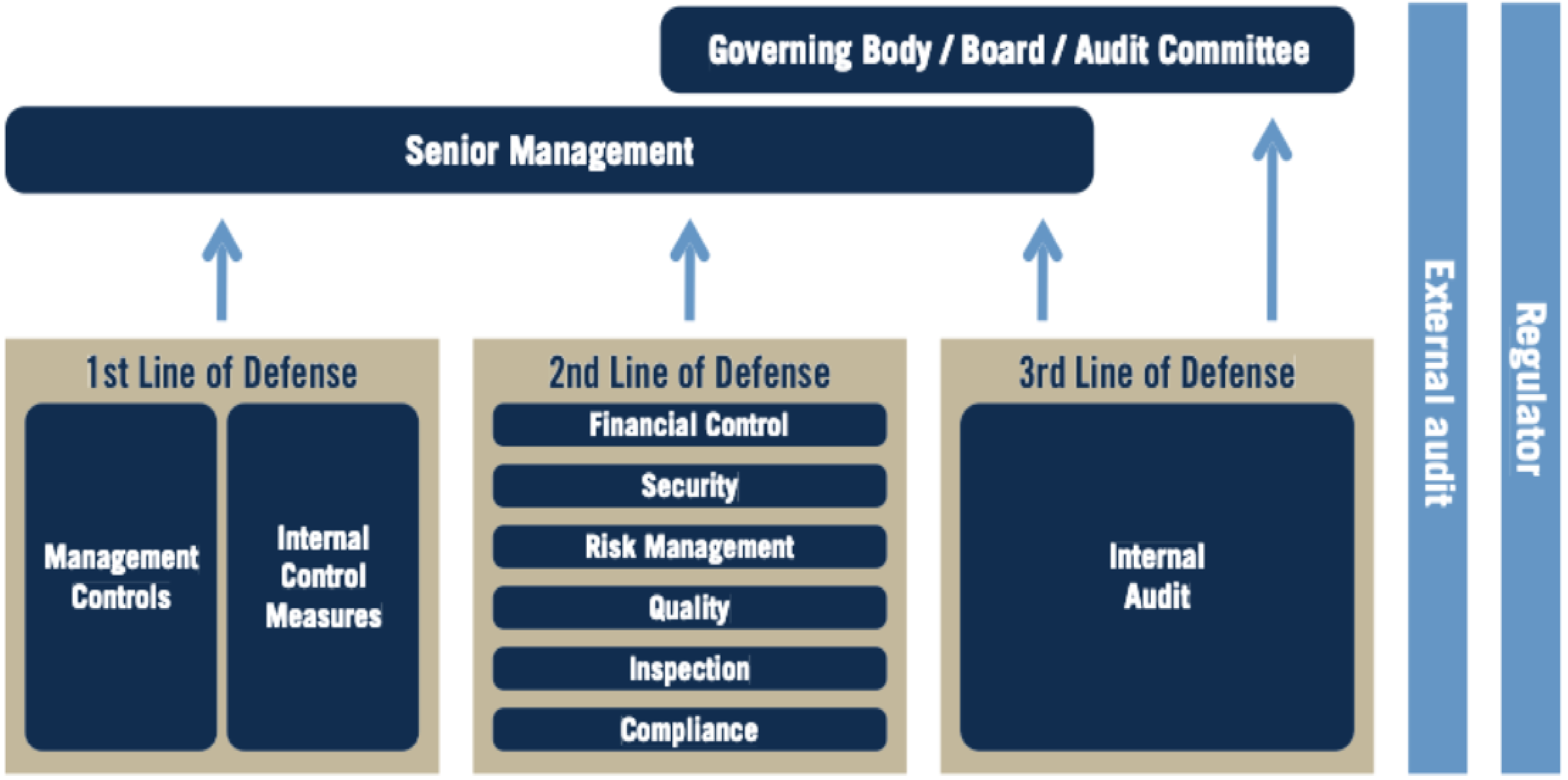
Board cyber legal responsibilities

❑ **Cybersecurity Program**: The Board of Directors sets the tone and direction for an institution's use of IT. The Board should approve the IT strategic plan, information security program, and other IT-related policies.

❑ **Audit**: The Board or its audit committee is responsible for reviewing and approving audit strategies (including policies and programs), and monitoring the effectiveness of the audit function.

❑ **Third Party Risk Management:** Board and senior management should establish and approve risk-based policies to govern the outsourcing process. The policies should recognize the risk to the institution from outsourcing relationships and should be appropriate to the size and complexity of the institution.

P3: CREATING THE RIGHT GOVERNANCE STRUCTURE FOR EFFECTIVE CYBERSECURITY IMPLEMENTATION



Governing Body / Board / Audit Committee

Senior Management

1st Line of Defense

Management Controls

Internal Control Measures

2nd Line of Defense

Financial Control

Security

Risk Management

Quality

Inspection

Compliance

3rd Line of Defense

Internal Audit

External audit

Regulator

P3: CREATING THE RIGHT GOVERNANCE STRUCTURE FOR EFFECTIVE CYBERSECURITY

❑ The three-line defense describes a governance model, setting up an optimal organizational structure to separate business, risk management and audit functions to effectively manage the cybersecurity risk emanating from the use of information technologies in business.

- ❑ **Functions that own and manage risks**
- ❑ **Functions that oversee risks:**
- ❑ **Functions that provide independent assurance**

P4: TOP DOWN APPROACH TO BUILDING A CULTURE OF SECURITY

- ❑ Cyber risk management requires a sincere commitment from the top management.
- ❑ The benefits of investing into cyber security is not very tangible and material.
- ❑ The tail end of the losses arising from the data and security breaches are difficult to measure.
- ❑ Without a top level commitment and its acknowledgement is the only way to instill cyber secure practices in the organization culture. Cybersecurity can't be implemented within silos in an organization.
- ❑ Since cyber security introduces friction within business units, it needs to be embedded into the Organisational culture . How?

P4: TOP DOWN APPROACH TO BUILDING A CULTURE OF SECURITY

❑ **Cybersecurity Awareness Program:**

❑ **Security by design" principle (SDP)**

❑ **Defense in Depth (DiD)**

P5: GIVE CYBER RISK MANAGEMENT REGULAR AND ADEQUATE TIME ON BOARD MEETING AGENDAS

- ❑ Boards should have frequent, timely discussions about cyber risks and may seek expertise beyond the confines of the boardroom.

Discuss how (5 Questions CII)

P5: GIVE CYBER RISK MANAGEMENT REGULAR AND ADEQUATE TIME ON BOARD MEETING AGENDAS

i. How are the company’s cyber risks communicated to the board, by whom and with what frequency?

ii. Has the board evaluated and approved the company’s cybersecurity strategy?

iii. How does the board ensure that the company is organized appropriately to address cybersecurity risks? Does management have the skill sets it needs?

iv. How does the board evaluate the effectiveness of the company’s cybersecurity efforts?

v. When did the board last discuss whether the company’s disclosure of cyber risk and cyber incidents is consistent with relevant guidance?

BOARD VIRTUAL OVERSIGHT OF CYBERSECURITY

❑ Organizations’ cyber-risk profile - Remote working, stress on the technology workforce, and looming expense pressures increase the potential for exposure.

❑ Cyber attacks could be business-ending events for organizations that are not prepared to defend themselves during a period in which funds to combat new cyber threats may have dried up or diminished.

❑ Board oversight is critical to ensuring that management is adapting to the evolving cyber-risk landscape as it works to maintain employee safety and continued business operations.

WHAT THE BOARD SHOULD KNOW

ICPAK
Credibility. Professionalism. Accountability

Rapidly Expanding Attack Surface

❑ This is driven by the need to deploy new equipment and technologies to support remote workers, such as virtual private networks and video conferencing and collaboration software.

❑ Requirements to relax controls and policies that were once relied on to protect enterprises in order to support remote working

WHAT THE BOARD SHOULD KNOW

Phishing.

- ❑ The risk of phishing attacks has increased now because remote workers may not have the full set of security defences normally available to them in their usual work environments
- ❑ Phishing is successful because it takes advantage of the responses people have to emotions elicited by an email

❑ Overworked Technology and Security Teams.

HOW SHOULD THE BOARD RESPOND?

Tactical

- ❑ Ensure the CISO/CIO/CTO understands that they have the support of the board to flag any **decision made in response to remote working** that may adversely impact enterprise cyber defence
- ❑ Ask for **periodic updates about cyberattacks** and incidents during the crisis. If there is nothing new to report, ask how the organization is validating that its monitoring protocols are working appropriately.
- ❑ Ask management if key **cybersecurity personnel** are being repurposed to handle operational technology tasks and, if so, when such personnel will resume their normal duties.

HOW SHOULD THE BOARD RESPOND?

Tactical

❑ Ask **what new equipment, technologies, and services** are being deployed in order to support response and relief efforts. Is there a process in place to validate that the cyber defences associated with these changes are being maintained?

❑ Ask **which security policies are being relaxed** in order to support the company’s response. Will these relaxed policies be in place for the duration of the crisis, or will more stringent policies be restored quickly? What risks do these changes create? Are these relaxed defenses being supervised?

HOW SHOULD THE BOARD RESPOND?

Strategic

Credibility. Professionalism. Accountability

Company-wide economic headwinds need to be considered as they may impact the budgeting of cyber defences.

- ❑ How is management considering the impact of furloughs and layoffs with respect to insider threat?
- ❑ What organizational restructuring actions might impact the company’s cybersecurity posture?
- ❑ Is the cybersecurity team proactively involved in the handling of these actions in order to mitigate and monitor any issues that arise?

HOW SHOULD THE BOARD RESPOND?

Strategic

- Understand the key cybersecurity scenarios that present the most material impacts to the enterprise. Consider, for instance, business interruption, data disclosure, and fraud.
- Define what risks the organization is willing to accept and to what degree.
- Understand how security changes driven by the current crisis will be monitored and improved over time and require updates on how these changes align with strategic objectives for cybersecurity.

HOW SHOULD THE BOARD RESPOND?

Strategic

- ❑ Establish mechanisms to provide continuous insight into the cost to recover from an attack and how an attack would interrupt the business.
- ❑ Develop an understanding of how your cyber-risk defence and exposure compares to peers in this environment.

QUESTIONS THE BOARD SHOULD ASK

- ❑ How is the IT function changing its strategic priorities in the short- , mid- and long-term and are resources sufficient to achieve these priorities?
- ❑ What security tools are being used to fortify the company’s network perimeter and thwart attacks?
- ❑ How are company policies and procedures related to remote access being strengthened to address the heightened risks created by employees working from home?
- ❑ Has the company kept its user access controls up to date in light of restructurings, furloughed employees and contractor changes?

QUESTIONS THE BOARD SHOULD ASK

- ❑ What policies and processes does the company have in place to ensure new technology tools and apps are properly vetted and approved for employee use?
- ❑ How secure are the board’s practices and technology tools used to communicate?
- ❑ What actions has the company taken to increase its detection and monitoring controls for identifying malicious activity on its systems?
- ❑ What actions has the company taken to educate employees—the first line of defence—about how to identify and react to the latest social engineering schemes?

QUESTIONS THE BOARD SHOULD ASK

❑ How is the IT function changing its strategic priorities in the short- , mid- and long-term and are resources sufficient to achieve these priorities?

❑ What security tools are being used to fortify the company’s network perimeter Applications and thwart attacks?

❑ How are company policies and procedures related to remote access being strengthened to address the heightened risks created by employees working from home?

❑ Has the company kept its user access controls up to date in light of restructurings, furloughed employees and contractor changes?

THANK YOU!

Vision: A world class Professional Accountancy Institute.