# Cyber Security Catalogue

## Information Protection and Business Resilience

*New ventures must be prepared to face fierce competition*

# KPMG CYBER SECURITY OVERVIEW

The constantly evolving threat landscape means that cyber risk is an everyday business consideration, in the same way that threats in the real world has always been. Cyber security is not a quick technical fix nor is it a matter solely for the IT department.

KPMG South Africa's Cyber Security team assists organisations in transforming their security, privacy and continuity controls into business-enabling platforms while maintaining the confidentiality, integrity and availability of critical business functions. The KPMG Cyber approach strategically aligns with our clients' business priorities and compliance needs.

## THE KPMG CYBER APPROACH

The KPMG Cyber approach is designed to be simple, effective and most importantly, aligned with the business needs of our clients.

Our services are segmented and supported by specialised teams, providing our clients with the right resources for any particular cyber-related need. Below is a breakdown of service offerings and our approach to cyber security:

### Prepare

Helping clients understand and improve their current state of preparedness against cyber -attacks, including services such as:

- Cyber Readiness Assessment
- Cyber Strategy and Transformation
- Cyber Governance and Resilience
- Data Governance and Privacy
- Emerging Technology Risk Assessment
- Threat Modeling
- Cyber Defence Architecture Design

### Protect

Helping clients design and implement their cyber defence infrastructure, including services such as:

- Identity and Access Governance
- Cloud Service and Cloud Provider Assessments
- Vulnerability Management
- Secure Application Development Services
- Data Leakage Prevention Services
- Critical Infrastructure Services
- Secure SDLC

### Detect & Respond

Helping clients maintain visibility of their cyber weaknesses, and respond to cyber attacks, including services such as:

- Cyber Operations and Incident Response
- Vulnerability and Penetration Testing
- Platform and Network Security Assessments
- Threat Detection and Intelligence Services
- Cyber Asset Inventory Services
- Post Breach Investigation

### Integrate

Helping clients embed cyber security into the culture and decision making of the organisation, including services such as:

- Cyber Security Awareness
- Cyber Incident Simulation
- Red Team / Blue Team Exercises
- Cyber in the Boardroom Services

Cyber Assurance Services incl. ISO, ISAE, PKI/NIST, etc.

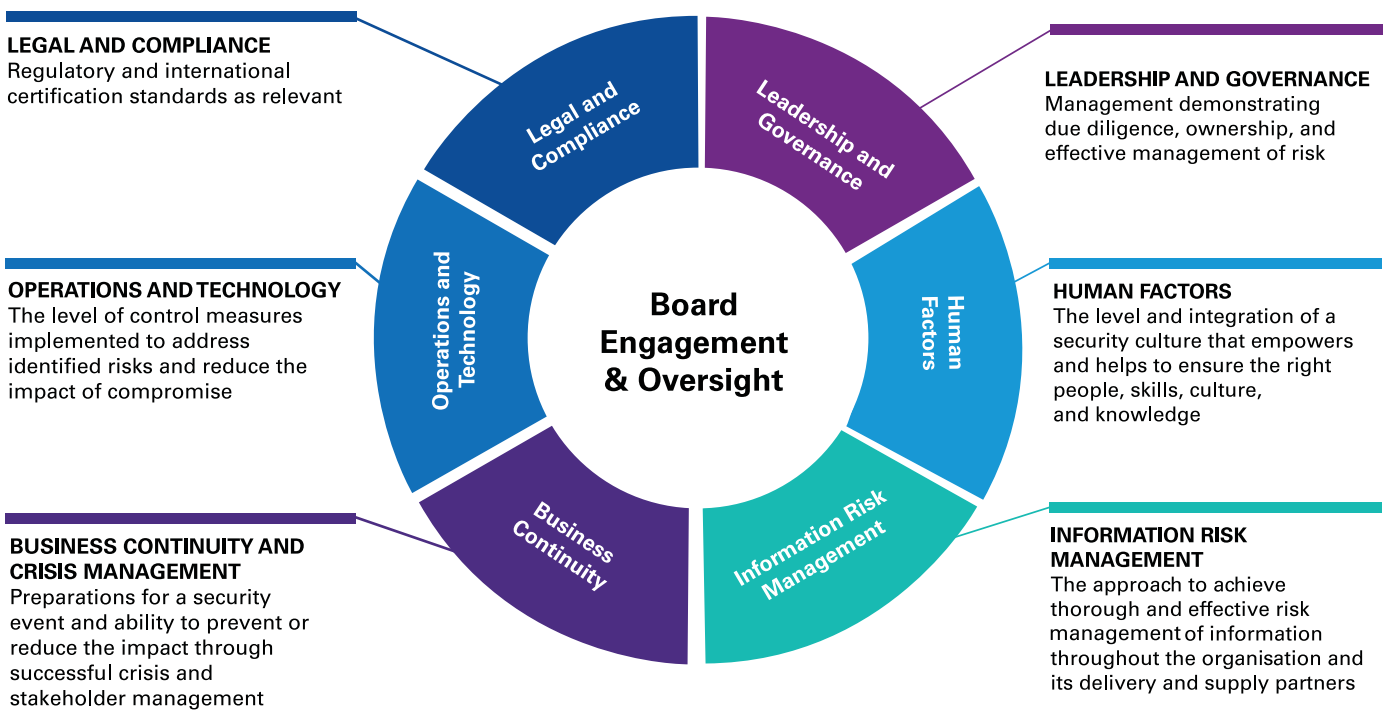
# CYBER READINESS ASSESSMENT

KPMG's Cyber Readiness Assessment (CRA) provides an in-depth review of an organisation's ability to protect its information assets and its preparedness against cyber threats. The cyber security landscape and the associated threats evolves at a rapid rate. The focus on cyber security is increasing accordingly, fuelled by the many high profile and highly disruptive/ damaging security breaches reported every day. As a result, organisations are subject to increasing amounts of legislative, corporate and regulatory requirements to show that they are managing and protecting their information appropriately. It is also increasingly common for government buyers and large corporates to demand confidence in information management as a qualifier for lucrative contracts or partnerships. With the stakes so high, organisations must decide on their cyber risk appetite and how they will respond. We can work with you to give you the advice and challenge you need to make decisions with confidence.

## WHAT IS A CYBER READINESS ASSESSMENT?

KPMG believes that we offer a unique service in the market that looks beyond pure technical preparedness for cyber threats. It provides a holistic view that analyses people, process and technology to enable clients to understand areas of vulnerability, to identify and prioritise areas for remediation and to demonstrate both corporate and operational compliance, turning information risk to business advantage.

In developing the assessment, KPMG has combined international information security standards with global insight of best practice in risk management, cyber security, governance and people processes. This global framework and approach provides a benchmarking view against your peers, and provides a modular and scalable approach that addresses **six key dimensions of an organisation's cyber readiness, as shown below:**



# CYBER GOVERNANCE AND RESILIENCE

Sooner or later any cyber defence will be breached. Organisations need to develop cyber resilience, a continuum of tested processes that enable it to respond appropriately to incidents of all sizes, including those which escalate and threaten the survival of the organisation itself. Focusing on technology alone to address these issues is not enough. Effectively managing cyber risk means putting in place the right governance and the right supporting processes, along with the right enabling technology. KPMG has assisted some of the world's largest organisations in defining the cyber governance strategies, and establishing the right controls and capabilities to be cyber resilient.

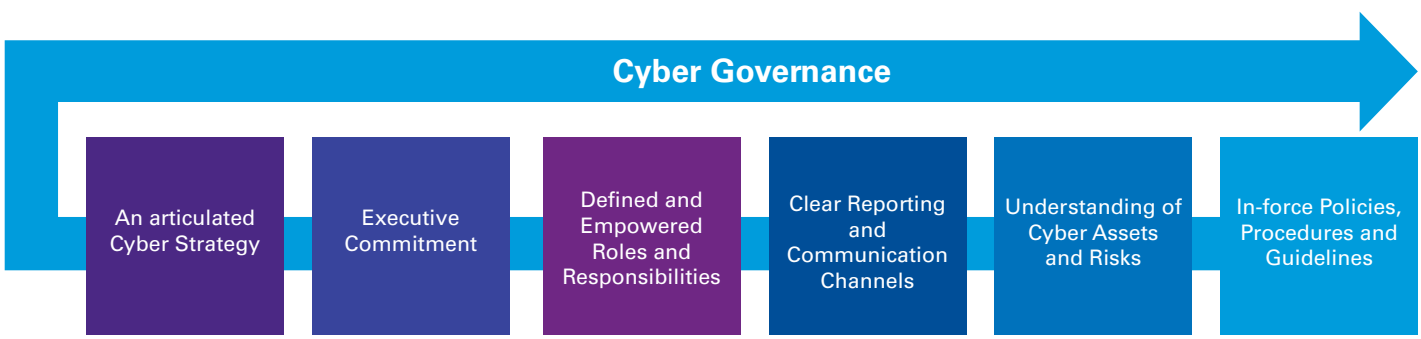
## KPMG'S CYBER GOVERNANCE AND RESILIENCE APPROACH

It is essential that leaders take control of allocating resources to deal with cyber security, actively manage governance and decision making over cyber security, and build an informed and knowledgeable organisational culture.

## KPMG'S APPROACH FOCUSES ON ADDRESSING KEY QUESTIONS THAT ARE TOP OF MIND FOR OUR CLIENTS:

- How big are cyber risks for our organisation and the organisations we do business with?
- Do governance processes and the organisational culture enable effective cyber risk management?
- Are we prepared to act in the event of a crisis or incident? Do we know how we should communicate and who should do it?
- Do we know which processes and/or systems represent the greatest assets from a cyber security perspective?
- Do our partners have the same risk appetite and cyber security measures as we do?

**Our Cyber Governance Health Check** identifies areas in which the board should act to improve its cyber risk management. KPMG will perform an assessment of the current Policies and Standards, Organisational Structure and Reporting Framework relating to cyber security based on leading practice standards and frameworks and provide a report highlighting the areas of concerns and provide recommendations for closing the gaps. Once priorities have been set, KPMG can assist clients in defining and developing their cyber security policies and standards, organisational structure and reporting metrics.



# DATA GOVERNANCE AND PRIVACY

Keeping data safe is no longer an afterthought at most organisations. Privacy has taken the global spotlight as we see mainstream organisations suffer severe reputational and financial damage resulting from information breaches. It is becoming increasingly relevant as organisations begin processing and extracting value from data in new ways through new technologies. Around the world, data protection and privacy legislation is increasingly important, and increasingly inconvenient. KPMG takes a business centric risk-based approach to Data Governance and Privacy, which focuses on both the technical and governance layers.

## WHAT'S ON YOUR MIND?

- Do we know what sensitive information we have, where it is stored, who has access to it, and how it is destroyed?
- Are we complying with the relevant regulatory and international certification standards?
- Are we spending our time and money in the right areas?
- Is the board demonstrating due diligence, ownership, and effective management of information risk?

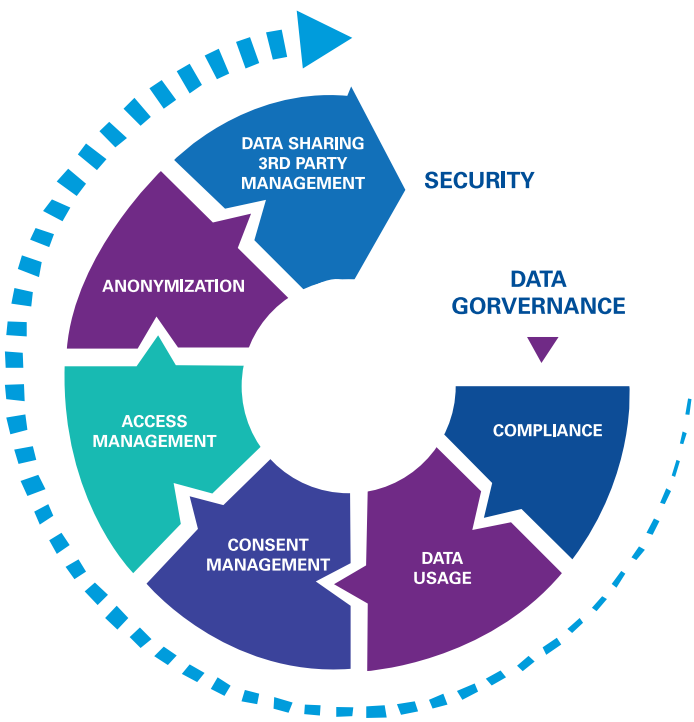
The information that an organisation possesses and uses is its most valuable asset. As data becomes more complex in today's digital era, it is ever more important that information usage and protection be transparent. Customers, regulators and partners demand data privacy. Good data governance reduces the risk of accidental and/or deliberate breaches of client information, employee data and/or intellectual property, and ultimately supports brand protection and increased enforcement of policies both internally and with third parties. In a world where data loss is heavily publicised and penalised, getting this right is proving financially significant, both financially and from a reputation standpoint.

## OUR APPROACH

*KPMG provides clients with assistance in two primary areas:*

- **Data Governance Processes:** KPMG supports clients in creating and implementing the appropriate policies and process while advising on third party management.
- **Technical Platforms:** KPMG advises our clients on the appropriate technical solutions for their needs, and partner with some of the leading solution providers to bring you the best capabilities.

We have identified eight high-risk focus areas highlighted in the diagram below, and offer guidance based on an augmented Data Governance life cycle to assist organisations in minimising risk and maximising control over data.



# EMERGING TECHNOLOGY RISK ASSESSMENT

Technology is playing a key role in capitalising on new business opportunities in an ever-competitive business world. We expect new global players to increasingly emerge and challenge market leaders. While the U.S. continues to be the tech leader, other countries vie for that position. Multiple versions of "Silicon Valleys" are springing up in tech hubs such as Tel Aviv, Shanghai, Tokyo, London, New York and Seoul as a tech economy builds with start-ups and innovations.

Cloud and mobile continue to power the shift to a new portfolio of emerging technologies: the Internet of Things, data & analytics and 3D printers, to name a few. The prospect of drones, digital currencies, robotics and artificial intelligence going mainstream adds a new dimension to the technology industry landscape.

As the scope of technology disruption increases, many new monetisation opportunities and business models are emerging. The rewards for embracing new technologies run deep, from productivity gains to cost efficiencies to quicker innovation cycles. Several risks loom large, however, with security remaining the biggest concern as technology companies continue to figure out how to prevent the growing number of hacking attempts and cyber-attacks that continue to make headlines.

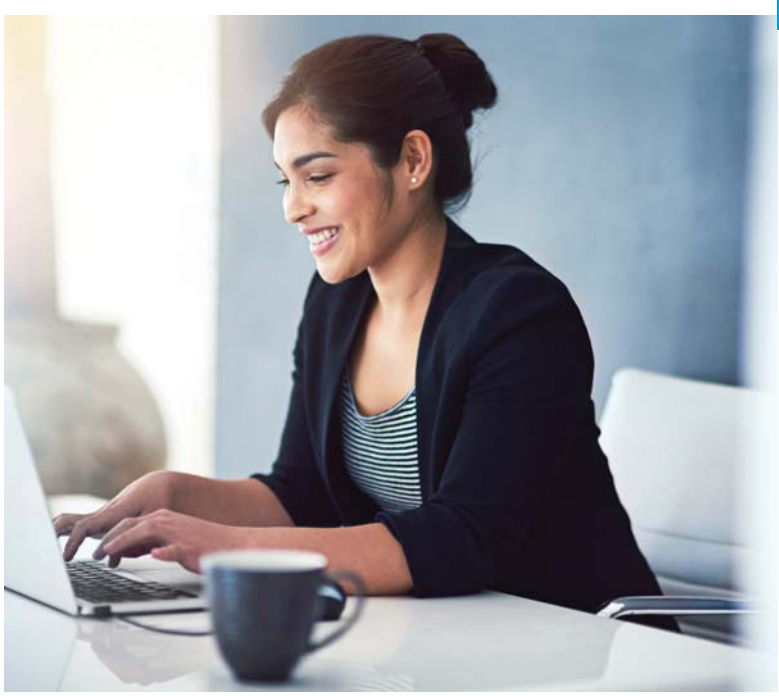
## OUR APPROACH

Our approach is to assist our clients to recognise and responsibly manage the enterprise wide risks resulting from the adoption and implementation of new and emerging technologies by performing the following:

- **Governance and Controls Review:** KPMG will review the governance processes and controls relating to access, secure development and configuration, and incident and change management.
- **Technical Security Assessment:** KPMG will perform a technical assessment aimed at ensuring that the infrastructure and security controls are implemented as designed and according to leading practice standards.

## WHAT'S ON YOUR MIND?

- How do we balance technology risks and rewards?
- Are we achieving tangible benefits from emerging technologies?
- Are we able to predict threats associated with new innovations?
- Do we understand emerging technologies well enough to protect your technology investments?



# THREAT MODELING

Cyber threats represent significant commercial and operational risk, yet many organisations do not know what threats they face, what their most crtitical cyber assets are, or who and what they are defending against. KPMG's Threat Modeling approach aligns to industry leading standards and frameworks, including OCTAVE, IRAM2, and ISO 27035 amongst others.

Cyber threats represent significant commercial and operational risk. Many enterprises are vulnerable to breaches, downtime and non-compliance and we understand your organisation, given its complex environments, company profile and pivotal importance to the South African economy may also be susceptible to these threats and attacks.

### WHAT'S ON YOUR MIND?

- Are we aware of the threats we face, both internal and external?
- Will my firm's existing combination of security controls protect against a sophisticated cyber-attack in practice?
- Are we extending our risk awareness to our supply chain and external vendors?

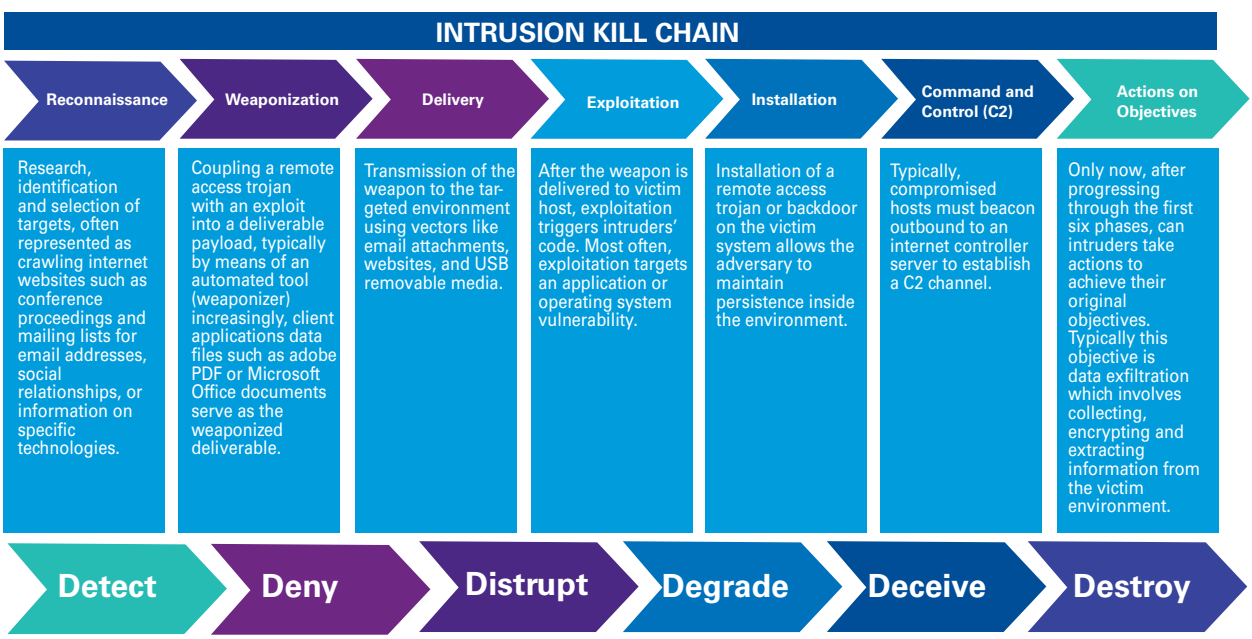
### OUR APPROACH

We leverage a structured approach to identify potential threats and vulnerabilities, along with the "cyber kill chain".

Our approach to threat intelligence reviews follows a two-phased approach, as described below:

- **IRAM2-aligned Threat Profiling Assessment:** KPMG will perform an analysis of your current cyber threat environment, information assets, threats profiles, vulnerabilities as well as the assets and associated threat events that could affect them utilising the IRAM2 methodology, from the Information Security Forum (ISF).

- **Attack Path Definition and Kill Chain Mapping:** KPMG will analyse the current cyber threat countermeasures implemented by the organisation, and map these against the threats and risks identified above, in order to map the events to attack paths. These models will then allow us to assess the capability to prevent, detect and respond to cyber threats using the Lockheed-Martin and Intel approach to the Intrusion Kill Chain.




*Ref: Lockheed Martin: Intelligence-Driven Computer Network Defense informed by Analysis of Adversory Campaigns and intrusion kill chain*

# SECURE SDLC

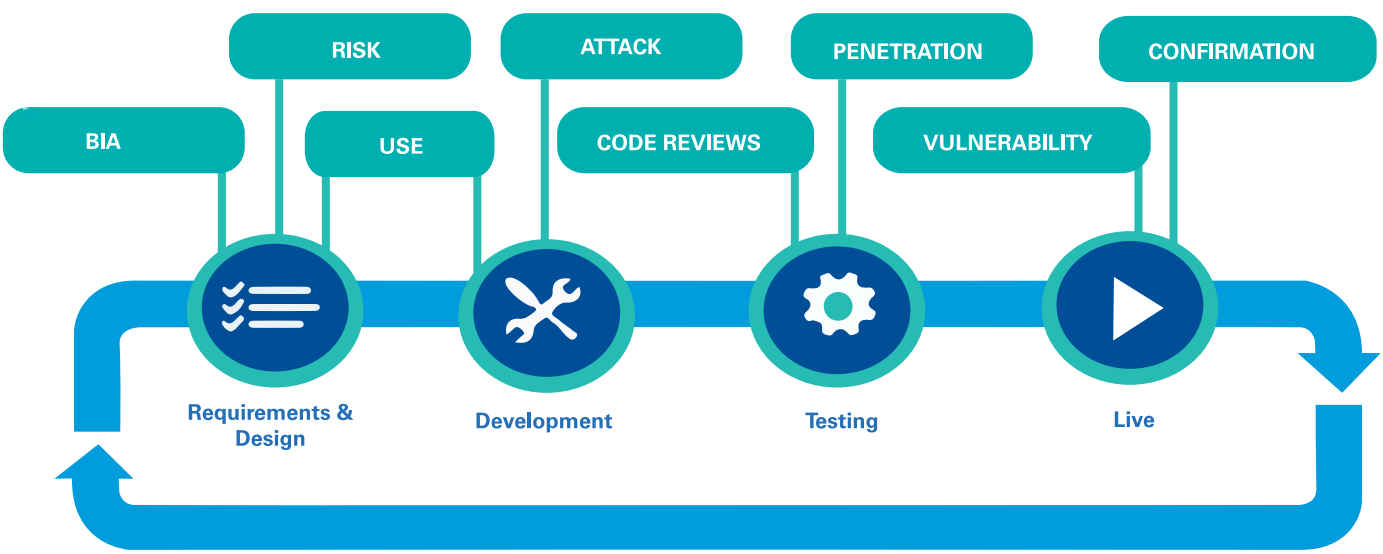
Most organisations have a well-oiled machine with the sole purpose to create, release, and maintain functional software. However, the increasing concerns and business risks associated with insecure software have brought increased attention to the need to integrate security into the development process. Implementing a proper Secure Software Development Life Cycle (SSDLC) is important now more than ever.

The use of the internet and network systems has become all pervasive and increases the risk for data integrity during software development. Instilling secure coding practices and controls within the development lifecycle can reduce software maintenance costs, decreases the number of security flaws and increases software reliability.

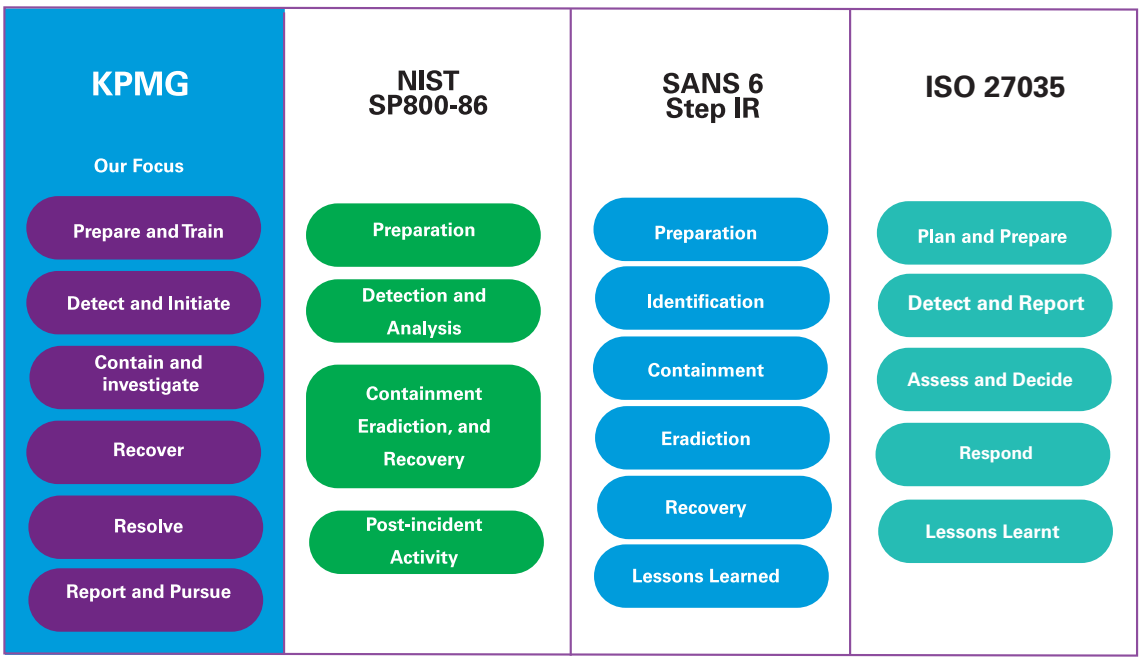
## OUR APPROACH

KPMG utilises a framework that encompasses the various aspects that organisations should be addressing, namely security policies and awareness, risk evaluations, security architectures, security assessment tools and software development methodologies with the aim to create a repeatable, auditable process that does not rely on after-the-fact inspections, in a way that best suits the team.

- **Requirements and Design:** Identify the business objectives and determine whether these align to the delivery of high quality systems, strong management controls and productivity
- **Development:** Conduct threat and risk assessments to identify potential threats and vulnerabilities in order to minimize the impact of attacks and assist in the development of risk-based test plans and use cases through defining actors, assets, services, roles and data sources etc.
- **Testing:** Conduct security testing including vulnerability assessments and penetration testing on software in a controlled environment to identify vulnerabilities. Perform code reviews and make recommendations based on software security best practices and the results of the review.
- **Live:** Vulnerability management to ensure that environmental scanning provides an accurate reflection of vulnerabilities and that there is adequate coverage of the attack.



# CYBER OPERATIONS AND INCIDENT RESPONSE SERVICES




In the unpredictable and fast-paced battle against cyber attackers, well-prepared incident response teams are a powerful weapon in an agency's arsenal. Responsible for assessing security systems and responding to security threats, incident response teams play a vital role in resolving issues and controlling damage of system breaches, malware exposure, and other security events.

Your organisation is notified by an external party that they believe your company may have been "hacked" and your customer data may be at risk. What do you do?

You have now confirmed that an unauthorised individual or team has gained access to your systems and data. You're not sure exactly what was accessed and what may have been lost. What next?

*Are you ready to manage a cyber- incident?*

**WHAT'S ON YOUR MIND?**

- Is our incident response and monitoring programs tuned to catch the attacks of today and not those of five years ago?
- If all security fails at some point, are we prepared to fail gracefully by having a defined incident response program?

# CYBER OPERATIONS AND INCIDENT RESPONSE SERVICES

**WHAT'S ON YOUR MIND?**

- The level of control measures implemented to address identified risks and reduce the impact of compromise?
- Why are we struggling to keep up with the requirements of fast-changing operational risk mandates?
- Does our monitoring process also identify risks to business?
- Are we extending our risk awareness to our supply chain and external vendors?

## OUR APPROACH

KPMG's approach to Cyber Response is created in in accordance with several international acceptable frameworks including NIST, ISO and SANS. Our approach is refined through real-word experiences with a focus on actionable results, rules of evidence and technical security experience.

- *Prepare and Train:* One of the most common causes of a failed response is lack of adequate preparation. KPMG can assist your organisation in establishing clear lines of communication, policies and procedures, and rules of engagement, in order to set the groundwork for a successful response if and when an incident occurs. In a parallel track, our teams work continuously to keep current on the latest technical methods, tools, and certifications for incident response.

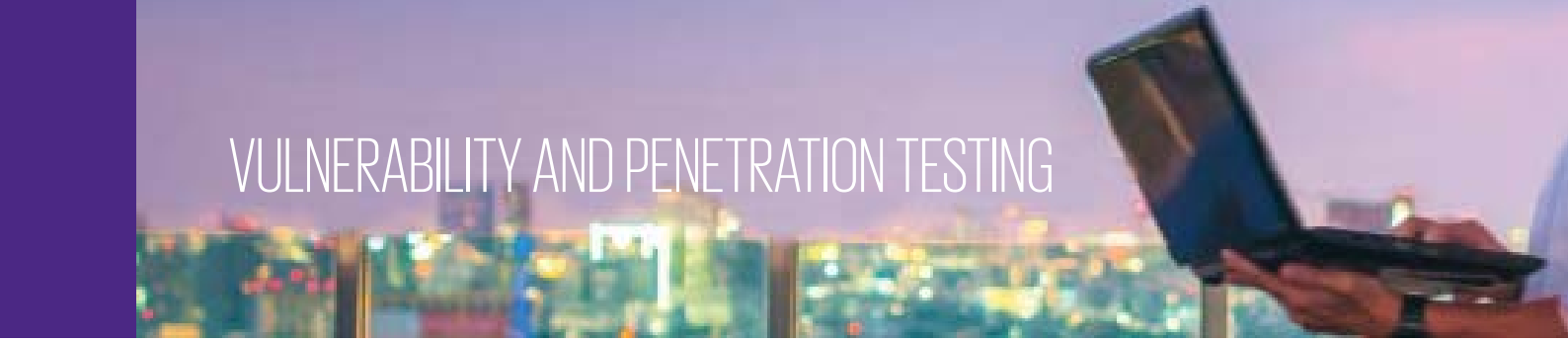
- *Detect and Initiate:* The trigger for this phase is a technical alert, an indication of fraud, or other communications from an outside entity such as law enforcement or an Internet service provider to your organisation. Our incident response professionals help execute plans created during the preparation phase and provide answers to pressing questions, such as: Have we been breached? Is the activity continuing? What are the potential damages? Do we need to begin notification and self-reporting?

- *Contain and Investigate:* During this phase, we help determine the source, method, and impact of the breach event, while attempting to assist you in limiting ongoing damage. These efforts are typically a balancing act between investigating and eradicating the threat. Responses can range from allowing the malicious actions to continue in order to facilitate evidence-gathering to an immediate suppression of malicious actions in order to limit damage.

- *Recover:* This phase consists of removal efforts that could not occur during the previous phases because of the potential impact on investigative efforts or prioritisation of other activities. The focus of this stage is to return the environment to normal operations.

- *Resolve:* A significant work stream during this phase is vulnerability assessment and penetration testing. This work may occur throughout the incident response process to support tactical efforts, and is followed by a more comprehensive process during this phase in order to determine the root causes of the malicious activity. This enables us to produce prioritised recommendations for improving the technical and governance environments, which can help prevent similar events from occurring in the future.

- *Report and Pursue:* The final phase consists of engagement reporting and may include ongoing support activities related to legal or civil pursuits of individuals or groups.



# VULNERABILITY AND PENETRATION TESTING

When a digital intruder accesses your network, they gain the ability to retrieve sensitive information and compromise your databases. The fallout may impact your business and its reputation. Information systems are one of the essential components of all the business processes, and in order to protect critical data and provide IT systems security it has become increasingly important to regularly evaluate the security of your computer systems and network. By simulating an attack from external and internal threats, KPMG can perform periodic assessments to provide an effective roadmap for protection of your business' critical information assets and address security threats before they are viable for a digital intruder.

KPMG can help better protect your business's critical and confidential information. With highly qualified and experienced professionals and proven tools, KPMG Vulnerability and Penetration Testing services provide objective and reliable solution according to your specific needs, with tactical and strategic security gap reports that support efficient closure of key vulnerabilities

## WHAT'S ON YOUR MIND?

- Can we reliably identify our vulnerabilities and reduce attack vectors available to digital intruders?
- Are we reliably addressing our key vulnerabilities?
- Are we able to detect when an attack is occurring?

## POTENTIAL BENEFITS TO YOU

- Identification of risks surrounding how the confidentiality of data may be compromised.
- Identification of poorly implemented security controls which may lead to performance and/or security issues.

## AFFORDABLE PIECE OF MIND

KPMG strives to offer you value, reasonable professional fees and an objective assessment of your network security controls. Our team offers an impressive track record and network of knowledge at your service. We have executed penetration tests for both small and large organisations with a wide range of network designs and information systems, across all key industry sectors.

## OUR APPROACH

KPMG's approach is based on the risks facing your organisation. Cyber attackers can target your network and eCommerce applications from the other side of the globe. Employees may also be attempting to compromise your confidential information. Thus, three types of penetration tests are available:

- **Vulnerability Assessment:** We use industry recognised vulnerability assessment tools such as Nessus, CyberArk and Acunetix to determine any vulnerabilities within the organisation, whether the vulnerabilities have been identified by the organisation's vulnerability management solution and whether the organisation is able to respond and remediate the vulnerabilities using a structured approach.

- **External penetration test:** We assess and quantify threats and vulnerabilities associated with specific target environments, such as Web servers, eCommerce sites, electronic mail servers and other publicly visible servers which could be targeted by cyber attackers.

- **Internal penetration test:** These help you focus on the protection of critical data and resources, intranet servers and databases and administrative level accounts. This type of test can identify risks which could be exploited by a disgruntled employee.

# SOCIAL ENGINEERING AND SECURITY AWARENESS

Every chain is as strong as its weakest link, and in cyber security this chain-link is often human. Employees with direct access to protected assets are usually the most obvious target for those with malicious intent to gain access to sensitive information. By-passing security controls via Social Engineering methods provides a low-cost and often stealthy way for attackers to breach defences and setup further and more advanced attacks. Taking these phenomenon into consideration, identification of the human risks and assessing the awareness level of the organisation are critical tasks that can't be postponed.

## OUR APPROACH

The assessment is performed by imitating the most common and effective attacks and techniques used by hackers and is designed to measure the efficacy of existing corporate security policies, security measures and employee training programmes.

*Our approach is broken up into three phases:*

- **Assessment of security awareness level- social engineering exercise:** Social engineering is a collection of attack methods and techniques, which exploit the deficiencies of user awareness. Illegal access to sensitive information, data leaks or other security breaches could be based on employees not knowing the contents of security policies, or not observing the rules.

Technological solutions do not provide complete security against social engineering attacks; the only one effective countermeasure is the improvement of security awareness. The best method to measure security awareness of an organisation's employees is to perform a social engineering exercise. In the course of our engagement, the current security controls will be tested by testing human factors, which will be completed by a number of techniques such as, dumpster diving, phishing attacks, impersonation via telephone and attempting to gain access to the organisations building.

- **Security awareness training:** After identifying security weaknesses emanating from human factors, the organisation can determine the requirements of security awareness, followed up by training for employees. Its purpose is to inform colleagues about the security policies and rules of the organisation and the necessity of observing them, as well as creating awareness of threats and attack types which target users.

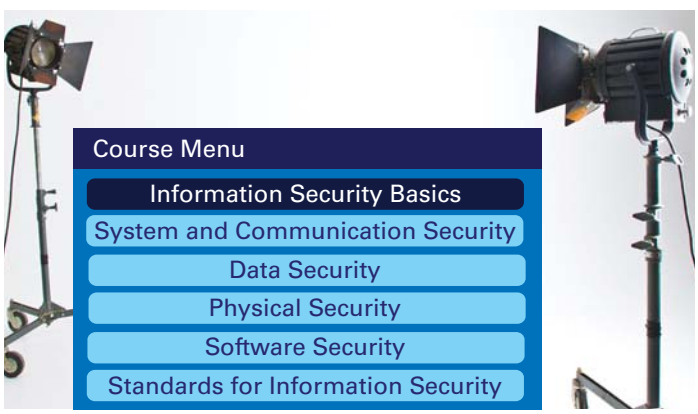
We recommend establishing our Training Programme at three levels: separate trainings for all users, for management and for the IT function. Specified training materials support participants in recognising the relevant threats and related security countermeasures.

- **Security awareness campaign:** Beyond assessing the level of users' security awareness and periodically organised awareness trainings, it is also important to sustain employees' awareness. The most effective method to achieve this is to organise a campaign, which can help remind employees every day of the most important security concerns.

*Possible elements of the campaign:*

- A fictional character or "comic book"-like series containing motivating messages
- Posters in the office promoting security awareness
- Screensavers highlighting human factor threats
- Tests, exercises and games.

### Example of KPMG's security Awareness



# CYBER INCIDENT SIMULATION

Your phone rings – sensitive information on your employees and your customers has been leaked – what do you do?

## ARE YOU READY TO MANAGE A CYBER INCIDENT?

We have observed through many high- profile examples, the answer to the question is unfortunately not well-known by organisations and the necessary reaction and response remain poorly understood.

While organisations can attempt to manage a crisis as it evolves, the likelihood of success of this approach is very low. This is often compounded by the use of untested incident response plans or poorly defined organisational responsibilities.

The challenge is that cyber threats are increasingly complex and their effects are readily amplified through social media and a 24-hour news cycle.

The frequency and severity of today's cyber incidents make them unlike any crisis your organisation has likely dealt with before.

Are you ready?

## WHAT IS CYBER INCIDENT SIMULATION?

KPMG's Cyber incident simulation service helps your organisation examine and understand its current incident response capabilities to better prepare for and manage cyber incidents.

With proven experience in incident response, crisis communications, operations and incident response planning, KPMG's cyber team will test and assess your people, your plans and processes by creating custom scenarios for you organisation that replicate the challenges of real cyber incidents.

This type of testing is an effective tool for your organisation to assess its current and desired state of incident preparedness and forms an important part of establishing your defensible position.

# CYBER INCIDENT SIMULATION

## OUR APPROACH

To assess, test and improve your organisation's ability to respond to a cyber- incident, KPMG uses a three step approach which can be customised to meet the needs of your organisation based on your current level of preparedness.

We will begin by working with you to obtain the necessary information on business processes and areas on concern that are essential for developing the exercises and simulation scenario.

*We then employ a combination of the following methods:*

- *Gamified workshop:* KPMG will facilitate a workshop for the organisations core operational and cyber security incident response team (CSIRT). KPMG will utilise our proprietary card-based game to simulate real world cyber security incidents and the responses available to mitigate them. This game features real world scenarios and solutions to gain insight into current cyber security threats. The game is played under the supervision of KPMG experts who will engage in discussion with your organisation around the concepts and threats that have been identified after the game has been played. This gamified workshop will identify the threats faced by your organisation, the opportunity of those threats arising and the current capabilities your organisation has to defend against the threats.

- *Paper- based simulation:* or your organisation's incident response plan and capabilities. This crisis scenario event will follow the full life cycle of an incident and the KPMG methodology will be utilised in order to evaluate the capabilities to mitigate the risks involved. Scenarios will range across business functions and assess your organisations full capabilities against cyber threats. During the test, KPMG's cyber team will work with you to review all elements of your current incident response plan and provide actionable recommendations to strengthen it.

- *Red team/ Blue team exercise:* A red/blue team exercise involves KPMG's Cyber Defence team simulating advanced attacks against your entire organisation. The blue team will be comprised of the organisation's staff who will be divided into a separate computer lab, modelled after your defence capabilities. These exercises comprise points based scenario attacks and will also utilise communication mediums to escalate and add a "real world feel" to these scenarios. Other mediums will include telephone calls, short message texts (SMS) and emails.

# THE KPMG DIFFERENCE

## THE KPMG DIFFERENCE

Having worked with major organisations from across various industries in South Africa and across the globe including financial services, healthcare and the public sector, KPMG's cyber team can help your organisation be cyber resilient with the end-to-end management of cyber security threats.

We can help your organization prevent, detect and respond to cyber threats.

## OTHER SERVICES

We understand the cyber threat landscape and the necessary actions your organisation needs to take to be in a defensible position.

**KPMG's Information Protection and Business Resilience (IPBR) team offers a range of services, including:**

- Data Loss (crown jewels, customer information, trade secrets)
- Identity and Access Management

## AWARD WINNING

KPMG International has been named a Leader in the Forrester Research Inc. Report. The Forrester Wave TM Information Security Consulting Services, Q1 2016.

The KPMG cyber team won the Information Security Consultancy award in 2011 and 2012. The team also won the MCA award in 2011 and 2012.

## INDEPENDENT

Our recommendations and technical strategies are based solely on what is fit and appropriate for your business. KPMG in South Africa is not tied to any technology or software vendor.

## TRUSTED

KPMG member firms have a long list of certifications and permits to work on.

- Business Continuity and IT Disaster Recovery Assessments and Implementation
- Privacy and POPI Assessments and Implementation
- IT Governance
- Information Security

To learn more about how we can help your organisation be cyber resilient, please contact us. In South Africa, we have 1 ISO 27001 Lead Auditor and 5 ISO 27001 Lead Implemeters.

## GLOBAL, LOCAL

KPMG is a global network of member firms with over 174,000 professionals in 155 countries with over 2,700 security practitioners globally, giving member firms the ability to orchestrate and deliver to consistently high standards worldwide. KPMG's regional practices can service your local needs from information security strategy and change programs, to low level technical assessments, forensic investigations, incident response, training and ISO27001 certification.

**Contact us | JHB**


**Jason Gottschalk**
National IPBR Lead
E: Jason.Gottschalk@kpmg.co.za
T: 082 719 1804

**Kaspar Euvrard**
Senior Manager
E: Kaspar.Euvrard@kpmg.co.za
T: 082 576 3588

**Mineshree Narsai**
Senior Manager
E: Mineshree.Narsai@kpmg.co.za
T: 082 716 8440


www.kpmg.com/za/cyber