# Cybersecurity Compliance Handbook for the Kingdom of Saudi Arabia

A starter's guide to comply with the Kingdom's national cybersecurity regulations

# About this handbook

During the past few years, several cybersecurity regulations have been introduced in the Kingdom of Saudi Arabia. This has resulted in a significant impact to government organisations and the Critical National Infrastructure in the Kingdom, resulting in many of them having developed cybersecurity programmes to meet the requirements of the regulations. We have put together this cybersecurity compliance handbook for business in the Kingdom to simplify the requirements and help you kick-start your cybersecurity compliance journey.

# Key steps to an effective cybersecurity programme

## Introduction to cybersecurity domains & key actions

In order to become compliant with national cybersecurity regulations in the Kingdom, number of key actions need to be taken across three pillars - governance, people, and technology:

**Governance** related actions that focus on organisational management and controls enforcement measures that are necessary to be cybersecurity compliant

**People** related actions that focus on cybersecurity measures that are necessary to be taken for human resources and human capital

**Technology** related actions that focus on the technical solutions, tools, and mechanisms that need to be implemented to be cybersecurity compliant

These actions are taken across several domains and sub-domains aligned to the national cybersecurity regulations within the Kingdom:

### Cybersecurity Governance

is the process of establishing organisational measures that ensure an entity's security programme aligns with business objectives, comply with applicable regulations, and achieve objectives for managing cybersecurity risk.

### Cybersecurity Defence

is the coordinated act of resistance that defends information, systems, and networks from cyber attacks by implementing protective processes and mechanisms to identify, analyse, respond, and report incidents that occur within a network.

### Cyber Resilience

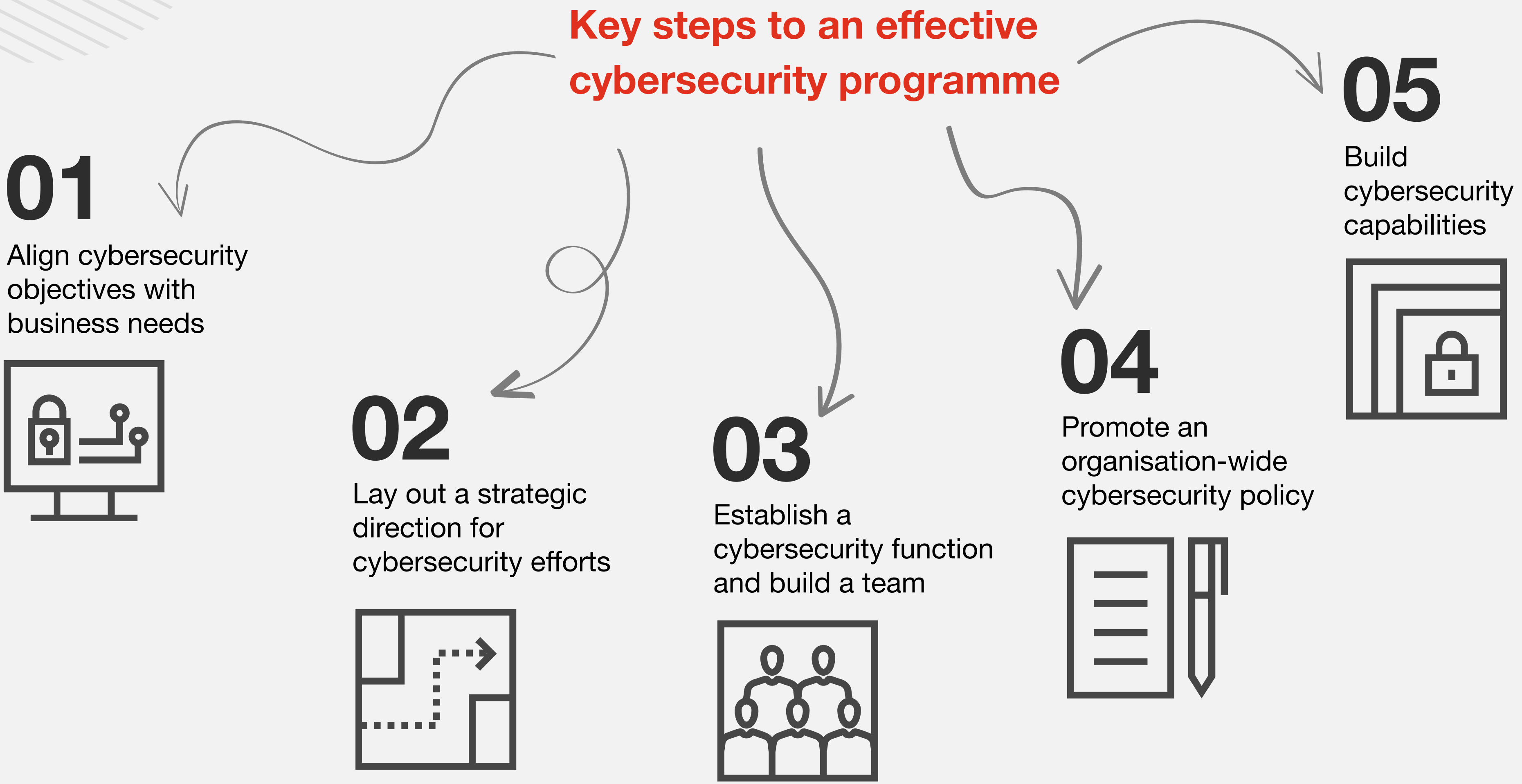
is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on information and technology assets.

### Third-party and Cloud Cybersecurity

is the process of enforcing cybersecurity measures to ensure the efficient management, monitoring and remediation of risks arising from the interactions and agreements with third-parties and cloud services providers (CSPs).

### Industrial Controls Systems Cybersecurity

is the ability to defend industrial controls systems (ICS) and operational technology (OT) by implementing protective security processes and mechanisms.



## Key steps to an effective cybersecurity programme

**01**

Align cybersecurity objectives with business needs

**02**

Lay out a strategic direction for cybersecurity efforts

**03**

Establish a cybersecurity function and build a team

**04**

Promote an organisation-wide cybersecurity policy

**05**

Build cybersecurity capabilities

Government entities in the Kingdom have set strategic and tactical objectives to strive towards achieving the Kingdom's Vision 2030. This includes the digital transformation of many core sectors and industries. The National Cybersecurity Authority (NCA) in the Kingdom has issued several cybersecurity regulations with which all government entities and the Critical National Infrastructure (CNI) must comply. As such, cybersecurity has become a core business mandate by all government entities and the CNI.

The cybersecurity compliance landscape is complex and evolving. It presents many challenges to organisations by creating additional overhead and uncertainty on many levels about how to be cybersecurity compliant.

All steps and actions taken towards an effective cybersecurity programme need to be aligned with the organisation and business needs, this includes:

- Understanding the business mandates, which will help define the scope of the cybersecurity programme within the organisation
- Understanding the strategic direction of the organisation, which will help lay out the strategic direction for cybersecurity (see step 2). The relationship and alignment between the business and cybersecurity can take many forms as seen in the below table.

| | Cybersecurity is an after-thought | Cybersecurity programme is aligned with the business need and objectives | | |
|---|---|---|---|---|
| **Cybersecurity Business Relationship** | **Impede** | **Support** | **Enable** | **Drive** |
| **Description** | Cybersecurity is an after-thought, and is a hindrance to the business objectives. The organisation's view on cybersecurity is that it purely impedes their activities. | Cybersecurity can identify opportunities to support the business objectives. Cybersecurity adjusts and responds to business needs. | Cybersecurity can identify opportunities to enable the business objectives. Cybersecurity introduces solutions to address the business need. | Cybersecurity can identify opportunities to drive the business objectives. Cybersecurity proactively introduces solutions that help shape business objectives. |
| **Example # 1** | Rejecting all cloud-based solutions | Restricting cloud-based solutions and requiring business justification | Incorporating cloud solutions through a cloud security framework & architecture | Introducing cloud-based security solutions to increase cyber posture |
| **Example # 2** | Blocking all removable media access (e.g. USBs) | Allowing limited removable media access requiring business justification | Introducing removable media security kiosks | Introducing automated and secure information sharing mechanisms |

## 01

**Align cybersecurity objectives with business needs**

## 02

Lay out
direction
cyberse

Align cybersecurity
objectives with
business needs

**02**

**Lay out a strategic direction for cybersecurity efforts**

03

Establis
cyberse
and bui

The organisation would be propelled towards fulfilling its goals following the development and enactment of a holistic cybersecurity strategy capturing its vision, mission, and goals. The organisation's vision & mission act as the catalyst for building a change-inducing strategy.

Consequently, in order to build an actionable plan for cybersecurity, the organisation should understand its current cybersecurity posture. This can be understood from a variety of perspectives ranging from current cybersecurity maturity, current cybersecurity risks, to technical vulnerabilities. The actionable plan should entail the actions as shown in the following sections (3 through 6) to detail the execution of the organisation's strategic objectives.

2

out a strategic
ction for
ersecurity efforts

03

**Establish a cybersecurity function and build a team**

04

Promote an organisation-wide cybersecurity policy

Establish a dedicated cybersecurity function that has the following characteristics:

- is independent from the IT function
- reports directly to the head of the organisation or their deputy
- is headed by a full-time qualified Saudi professional

Establish an independent cybersecurity steering committee or incorporate cybersecurity committee mandates within an existing committee (e.g. organisation GRC committee) reporting directly to the head of the organisation. This is to ensure leadership support in the implementation of cybersecurity requirements across the organisation.

3

lish a
rsecurity function
uild a team

Build
cybersecurity
capabilities

## 04

### Promote an organisation-wide cybersecurity policy

It is crucial for any organisation to create a comprehensive cybersecurity policy that addresses the challenges from the constantly evolving threats and the complex compliance requirements. The cybersecurity policy should ensure that the organisation can coordinate and enforce an organisation-wide cybersecurity program that promotes and communicates cybersecurity requirements internally to all the organisation's departments and externally to third-parties including suppliers and service providers.

In order to be effective, the organisation must first identify the relevant cybersecurity controls required for the protection of its business, operations and people. This should include high-level requirements in the cybersecurity policy, with supporting cybersecurity technical standards, procedures, frameworks, and guidelines. Additionally, these cybersecurity requirements need to be documented, approved, communicated, and regularly reviewed periodically or when changes are required by the cybersecurity function. In fact, the cybersecurity function has an important role to ensure that cybersecurity requirements are communicated, implemented and reviewed within the organisation.

04

Promote an organisation-wide cybersecurity policy

## 05

**Build cybersecurity capabilities**

Plan risk and compliance requirements

Embed security into people processes

Nurture a cyber-aware culture

Govern identity & manage access

Know & protect data

Protect information and technology systems

Secure electronic communications

Build & maintain secure applications

Safeguard mobile devices

Fortify the network

Defend operational technology

Guard facilities & assets

Manage vulnerabilities and weaknesses

Identify potential exposures with penetration testing

Monitor & detect cybersecurity threats

Enrich cybersecurity operations with threat intelligence

Respond to cybersecurity incidents

Develop recovery plans & ensure service continuity

Manage & safeguard cloud hosting

Embed security into third-party agreements

# Plan risk and compliance requirements

## Documentation

- Develop a cybersecurity policy that contains cybersecurity risk management requirements including developing a cybersecurity risk management methodology and process with defining the triggers for conducting risk assessment.

- Develop a cybersecurity policy that contains cybersecurity compliance requirements including defining the cybersecurity national and international regulations the organisation needs to comply with.

- Develop a plan to conduct periodic cybersecurity self reviews and audits across the organisation to assess the compliance with cybersecurity policies and regulatory requirements.

- Develop a plan to conduct yearly cybersecurity reviews and audits by an independent party from the cybersecurity function to assess the compliance with cybersecurity policies and legal and regulatory requirements.

## Technology

- Implement a Governance, Risk & Compliance (GRC) tool to enable your organisation in performing and integrating governance, risk management, and compliance processes effectively.

## Responsibilities

- The cybersecurity department conducts cybersecurity risk assessments and monitors the implementation of the risk mitigation plans within the organisation.

# Embed security into people processes

## Documentation

- Develop a cybersecurity policy that contains human resources (HR) security requirements that defines and enforces personnel cybersecurity controls required prior to employment, during employment and after termination.

- Develop employee contract templates including cybersecurity responsibilities and non-disclosure clauses.

- Develop a process to screen candidates for cybersecurity and privileged positions.

## Responsibilities

- The cybersecurity department monitors the implementation of the cybersecurity requirements throughout the employees' lifecycle.

# Nurture a cyber-aware culture

## Documentation

- Develop a cybersecurity awareness program that covers multiple channels to nurture a risk-aware cybersecurity culture and strengthen the awareness of individuals about cyber risks and threats.

## Technology

- Implement and configure a Learning Management System (LMS) to deliver cybersecurity awareness content including courses, short videos, flyers, publications and news.

- Implement and configure a phishing simulation tool to conduct periodic phishing assessment on employees, contractors and third-parties.

## Responsibilities

- The cybersecurity department develops and delivers cybersecurity awareness content and periodically measures the awareness level across the organisation.

# Govern identity & manage access

## Documentation

- Develop a cybersecurity policy that contains identity and access management security requirements and specifies how access is managed and who may access information under what circumstances.

- Develop a password policy to define the way passwords are created, the complexity requirements, secure storage, safe transmission, periodic randomization, prompt deprovisioning, continuous monitoring, and more.

- Develop secure log-on procedures to control access to systems and applications and prove the identity of the user.

- Develop standards that include technology-specific access control requirements.

## Technology

- Implement an access management solution that provides the ability to manage and monitor user access rights and permissions to ensure that only authorised users have access to the organisation's resources based on their job role, their department or any other attributes that seem appropriate.

- Implement a Privileged Access Management (PAM) solution that provides monitoring and management of privileged access to critical assets and business resources across the organisation's environment. PAM is grounded in the principle of least privilege, wherein privileged users only receive the minimum levels of access required to perform their job functions.

- Implement a VPN solution that allows users to establish a secure, encrypted network connection to internal resources while connecting over public or insecure networks, and ensure that multi-factor authentication is enabled on the VPN as an additional layer of defence to prevent misuse and theft of credentials.

## Responsibilities

- The cybersecurity department monitors and reviews the identity and access management logs

# Know & protect data

## Documentation

- Develop a cybersecurity policy that contains data and information protection requirements covering data and information ownership, privacy, classification and labelling mechanisms ensuring the confidentiality, integrity and availability of the organisation's data and information.

- Define data owners for all data types within the organisation. Define a data classification scheme to establish sensitivity categories on data such that security controls can be applied based on the classification.

- Define a flexible (physical or digital) cybersecurity labelling mechanism streamlining and simplifying delivery of necessary information.

- Develop a data and information privacy plan to employ organization-approved procedures to maintain the integrity of, and control the accessibility to, the organization's restricted data where data undergoes processing, storage, and transmission.

- Develop a cryptography policy that contains cybersecurity requirements covering secure key management and encryption of data in-transit and at-rest, ensuring the proper and efficient use of cryptography to protect information assets.

- Define an approved cryptographic solution standard covering technical and regulatory requirements.

## Technology

- Deploy a data discovery and classification solution that scans data repositories for the types of data considered important, based on industry standards or custom requirements (such as Payment Card Industry Data Security Standard, General Data Protection Regulation, Intellectual Property) sorting it into categories and clearly labelling it with a digital signature denoting its classification.

- Configure and implement an external device encryption solution to fully encrypt external storage media devices such as external hard drives, and USB flash drives. Protection of data housed within these devices is secured without access to the key and encryption software.

- Implement an endpoint encryption solution fulfilling full disk encryption and covering encryption of all data such as files, folders, and the operating system. This type of encryption is useful in the absence of un-assured physical security of the system.

## Responsibilities

- The cybersecurity department defines the required cybersecurity controls for each data classification level and ensures proper data protection controls are in place to protect each level based on the data's criticality.

# Protect information and technology systems

## Documentation

- Develop a cybersecurity policy that contains cybersecurity requirements for asset management, which includes managing information assets throughout their lifecycle from creation to usage to disposal.

- Develop and maintain an asset register for the entire organisation, which has a list of all the information assets that the organisation owns.

- Develop and maintain an information asset lifecycle procedure, which includes how information assets are created, maintained, and destroyed in the organisation. This ensures asset-related procedures are documented and made aware to all respective stakeholders.

- Develop and maintain standards and procedures that include technology-specific asset requirements for specific information assets that require special care and consideration; this includes onboarding and destruction of assets and asset classification.

- Develop and maintain security hardening standards to set a baseline of requirements for each information system and information processing facility (including workstations and infrastructures).

## Technology

- Implement and configure an asset discovery and visibility tool to eliminate shadow IT and detect any rogue assets.

- Implement and configure a Configuration Management Database (CMDB) to document all the relevant hardware and software components of the organisation’s information assets and mantain an automated register.

- Deploy an end-point security solution to help detect, analyse, block and contain malicious activity on endpoint devices, and ensure that the solution includes APT protection capabilities that protects against advanced malware, zero-day attacks and persistent attacks.

- Obtain a patch management solution that automates, manages, and regularly installs missing patches on software applications. A patch management solution will also minimise the possibility of system crash or compromise due to an outdated or defective software.

## Responsibilities

- The cybersecurity department monitors and reviews the organisation’s assets’ security logs including the information systems and information processing facilities’ security logs.

# Secure electronic communications

## Documentation

- Develop a cybersecurity policy that contains cybersecurity requirements for electronic communication security that details the acceptable use of the corporate email system and other electronic communication means.

- Develop standards that include technology-specific email security requirements for specific users or category of users that require special care and consideration.

## Technology

- Obtain and install an email security solution that is able to detect and block unwanted emails such as spam or phishing emails. The solution should also have Advanced Persistent Threat (APT) protection capabilities to protect against advanced threats and zero-days, as well as Sender Policy Framework to protect against spoofing. If there is a requirement to use webmail remotely, multi-factor authentication should be enabled.

- Backup and archive emails utilising a solution that stores and preserves emails in a secure manner and provides the ability to restore the emails whenever necessary.

## Responsibilities

- The cybersecurity department monitors and reviews the email security logs and ensures email security requirements are in place.

# Build & maintain secure applications

## Documentation

- Embed cybersecurity requirements in project management and change management procedures, which should include the following requirements: vulnerability management, configuration assessments, security compliance testing, secure integration, hardening and patching.

- Adopt secure coding standards to be followed while developing in-house applications.

- Develop a cybersecurity policy that contains application security requirements such as web application firewall, multi-tier architecture, secure protocols, and multi-factor authentication requirements.

- Develop a secure usage policy and publish it to users within the organisation.

- Develop technology-specific application security standards.

## Technology

- Implement and configure a **web application firewall (WAF)** that protects web applications from a variety of application-layer attacks. A WAF solution filters, monitors, and blocks any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorised data from leaving the app.

- Version control system.

- Implement a static or dynamic application security testing software (SAST/DAST) to find security vulnerabilities within the application source code.

## Responsibilities

- The cybersecurity department conducts configuration reviews, vulnerability assessments and compliance tests as part of the project management/change management lifecycles.

# Safeguard mobile devices

## Documentation

- Develop a cybersecurity policy that contains mobile device and bring your own device (BYOD) security requirements to enforce data encryption on business and personal devices and define secure wiping process upon employee termination.

- Develop a cybersecurity policy that contains mobile device security requirements covering separating, secure archiving/wiping, and encrypting of data and information stored on mobile devices and Bring Your Own Device (BYODs) satisfying protection from cyber risks and securely handling sensitive information while utilising BYOD.

## Technology

- Configure the mobile device management (MDM) solution to enroll and provision devices remotely with corporate network settings (such as VPN and Wi-Fi restrictions). Also, allows moderation and restriction of features such as account modification, roaming, cellular data control, pairing, and more whilst allowing a certain level of flexibility for regulated BYOD.

## Responsibilities

- The cybersecurity department monitors the implementation of the cybersecurity requirements for the use of mobile devices across the organisation.

# Fortify the network

## Documentation

- Develop a cybersecurity policy that contains network security requirements that outlines guidelines for computer network access.

- Develop standards that include technology-specific network security requirements.

## Technology

- Install an internet proxy (also known as forward or web proxy) to act as a gateway between a client application, for example, a browser, and the internet. It examines the data going in and out of the client or network before applying correspondent rules.

- Implement next-generation firewalls (NGFWs), which are considered as deep-packet inspection firewalls that move beyond port/protocol inspection and blocking, to add application-level inspection and control and integrated intrusion prevention. A dedicated Intrusion Prevention System (IPS) provides signature-based threat detection to proactively detect an intrusive activity and attempt to stop it before it reaches the targets.

- Use DNS security and DNS filtering to block malicious websites and filter out harmful or inappropriate content as a countermeasure to address cyber-attacks where hackers use DNS to distribute malware, communicate with compromised systems, and exfiltrate data.

- Synchronize servers to a centralised NTP source that synchronizes the time of a computer client to a centralized, trusted source in order prevent the manipulation of time information by attackers.

## Responsibilities

- The cybersecurity department monitors and reviews the network security logs.

# Defend operational technology

## Documentation

- Develop a cybersecurity policy that includes the physical and logical security requirements related to Industrial Control Systems (ICS).

## Technology

- Implement and configure the necessary cybersecurity technologies while considering those qualified by the entities' OEMs.

## Responsibilities

- The ICS cybersecurity department (if applicable to the organisation) ensures the protection of the industrial control systems by monitoring the implementation of the ICS cybersecurity controls.

# Guard facilities & assets

## Documentation

- Develop a cybersecurity policy that contains physical security requirements to safeguard the facility such as requirements of authorised access to sensitive areas, CCTV monitoring, protection of surveillance records, secure destruction of assets, and security of the organisation's devices.

## Technology

- Implement and configure physical access control solutions (detective, preventative or deterrent) to control the ability of people or other assets to enter a protected area by means of authentication and authorization at access control points. All facilities owned or operated by the organisation should be protected.

- Enable video surveillance by installing IP-based CCTV cameras to optimise security monitoring by recording events, retaining records, and integrating with other security solutions for alerting and reporting.

- Degausser magnetic storage media to safely erase the drive and destroy classified data.

## Responsibilities

- The cybersecurity department monitors the implementation of the cybersecurity requirements for physical security.

# Manage vulnerabilities and weaknesses

## Documentation

- Develop a cybersecurity policy that includes vulnerability management requirements for assessing, identifying, classifying, managing, and remediating vulnerabilities. This policy shall be documented, approved, communicated, implemented and regularly reviewed based on planned intervals or when changes are required.

- Develop a vulnerability management standard to define the processes and procedures of assessing, remediating and reporting vulnerabilities.

- Develop a vulnerability classification methodology to classify system defects based on their criticality and associated risks as per the risk management methodology.

- Develop a plan for conducting vulnerability assessments periodically to review, identify and classify security issues within the organisation’s systems and apply appropriate remedial actions.

## Technology

- Procure and configure a **Vulnerability Assessment Tool** that scans and reviews networks, applications and systems to evaluate their susceptibility to known weaknesses and vulnerabilities, and provides mitigation measures as and when necessary.

## Responsibilities

- The cybersecurity department conducts vulnerability assessments regularly for the organisation's information assets.

# Identify potential exposures with penetration testing

## Documentation

- Develop a cybersecurity policy that includes penetration testing requirements for conducting penetration tests and evaluate the security of the organisation’s systems to spot and identify potential exposures.

- Develop a penetration testing standard to outline the procedures of conducting the tests, defining the approach and attack scenarios.

- Develop a plan for conducting penetration testing periodically to ensure evaluating the organisation’s system security and detecting exploitable vulnerabilities.

## Technology

- Leverage a collection/suite of penetration testing tools to assist the tester in conducting attack scenarios and uncover vulnerabilities in networks, applications and end-points.

## Responsibilities

- The cybersecurity department conducts penetration testing regularly for the organisation's information assets.

# Monitor & detect cybersecurity threats

## Documentation

- Develop a cybersecurity policy that contains event log and monitoring management requirements to reduce potential security breaches through ensuring continuous monitoring, timely detection and analysis of security events.

- Develop a standard of cybersecurity event logs and monitoring management to define the event logging, log format, event sources, events monitoring, alerting, event log review and logs' retention etc.

## Technology

- Integrate a **Security Information and Event Management (SIEM)** solution that provides a holistic view and real-time monitoring of an organisation's security posture by aggregating event logs from different information systems in order for security teams to detect and manage security events.

## Responsibilities

- The cybersecurity department oversees the activation of event logs on the organisation's critical systems, remote access and privileged user accounts. This is to continuously monitor and analyse events for early detection of cyber attacks.

# Enrich cybersecurity operations with threat intelligence

## Documentation

- Develop a cybersecurity policy that includes threat management requirements to ensure the organisation manages threats and having adequate protection through identifying and analysing undetected and potential cyber threats in terms of threat actors, their motive and capability, threat vectors, and attacks.

- Develop a standard for threat management to define the appropriate threat intelligence feed's maintenance.

## Technology

- Subscribe to a reputable threat intelligence feed to allow security decision makers to focus on threats that matter now, reduce threats from fast-changing actors, detect emerging attacks and reduce existing organisational threat risk surface. Connect security solutions to external threat intelligence feeds to receive actionable intelligence, advanced analytics, Indicators of Compromise (IoCs), Indicators of Attack (IOAs), and reports on potential attacks.

## Responsibilities

- The cybersecurity department collects and analyses threat intelligence feed and defines cyber threats and actors' tactics, techniques and procedures.

# Respond to cybersecurity incidents

## Documentation

- Develop a cybersecurity policy that includes incident management requirements to ensure proper and timely response to and reporting of cybersecurity incidents.

- Develop incident response playbooks to provide guidance in developing incident response, recovery and business continuity plans, and defining incidents' classification and prioritisation and incident reporting.

- Develop an incident response plan to properly identify, eliminate, and recover from cybersecurity incidents.

## Technology

- Implement an **Incident Management Platform** to automate, guide and assist the incident response process. The system helps the security analyst by providing incident case management, Integrated SIEM and other tools and automated response using security playbooks.

## Responsibilities

- The cybersecurity department detects, analyses and responds to cyber incidents and ensures reporting cybersecurity incidents to National Cybersecurity Authority (NCA).

# Develop recovery plans & ensure service continuity

## Documentation

- Develop a cybersecurity policy that includes cybersecurity aspects of business continuity to ensure continuity of systems and procedures after security incidents.

- Develop a cybersecurity policy that contains backup and recovery requirements to retain records and software, establish frequency of backups based on the volatility of data, and have one fully recoverable version stored in a secure off-site location.

- Develop a regular testing of backup plans or after any significant change in processes or procedures.

- Develop a failover strategy backing the primary system in case of failure and allowing the resumption of system availability when failover mechanisms have been unable to keep the system available.

- Develop a disaster recovery plan (DRP) and incident response plans to detail how to respond to unplanned incidents such as cyber attacks, natural disasters, power outages, and more. The DRP outlines strategies on how to minimize the effects of a disaster, allowing the organization to quickly resume key operations or operate as if no disaster occurred.

## Technology

- Implement **redundant information processing facilities** to ensure that in the event of a disaster, work does not get halted completely, which may translate into the organisation suffering significant losses.

- Implement a backup management system to maintain a copy and archive important data and protect it from accidental data loss, corruption, and unauthorised access.

## Responsibilities

- The cybersecurity department ensures cybersecurity requirements and cyber attacks are included within the business continuity and disaster recovery plans/strategies.

# Manage & safeguard cloud hosting

## Documentation

- Develop a cybersecurity policy that includes the security requirements related to cloud computing and hosting.

## Technology

- Implement and configure the necessary cybersecurity technologies.

## Responsibilities

- The cybersecurity department ensures the organisation's cloud environment is protected by monitoring the implementation of the cloud security requirements.

# Embed security into third-party agreements

## Documentation

- Develop a cybersecurity policy that contains third-party security requirements for contracting with third-parties and managed services.

- Embed cybersecurity requirements in service-level agreements (SLAs) such as non-disclosure clauses, secure removal of organization’s data by third parties upon end of service, incident communication procedures and cybersecurity compliance requirements.

## Responsibilities

- The cybersecurity departments ensure that cybersecurity requirements are embedded within SLAs.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 156 countries with over 295,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for 40 years, PwC has 22 offices across 12 countries in the region with around 7,000 people. (www.pwc.com/me).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

# Contact us

### Haitham Al-Jowhari
Partner, Cyber Security
haitham.al-jowhari@pwc.com
+966 54621 8888

### Mohammed Ayesh
Director, Cybersecurity
mohammed.ayesh@pwc.com
+966 54767 7828

### Ali Mouslmani
Senior Manager, Cybersecurity
ali.mouslmani@pwc.com
+971 54793 4058

### Abdulrahman Kurdi
Manager, Cybersecurity
abdulrahman.kurdi@pwc.com
+966 54766 8395