Hacktales

CYBERSECURITY FOUNDATION PROGRAM

Authors:
Chikodili Udeh & Jide Adebayo

Contents

Hacktales

01

Human Factors

- Facts and Findings
- Psychology of human error
- Human Factor Strategies

02

Security Governance

- Governance Structure
- Compliance
- Cybersecurity Policies

03

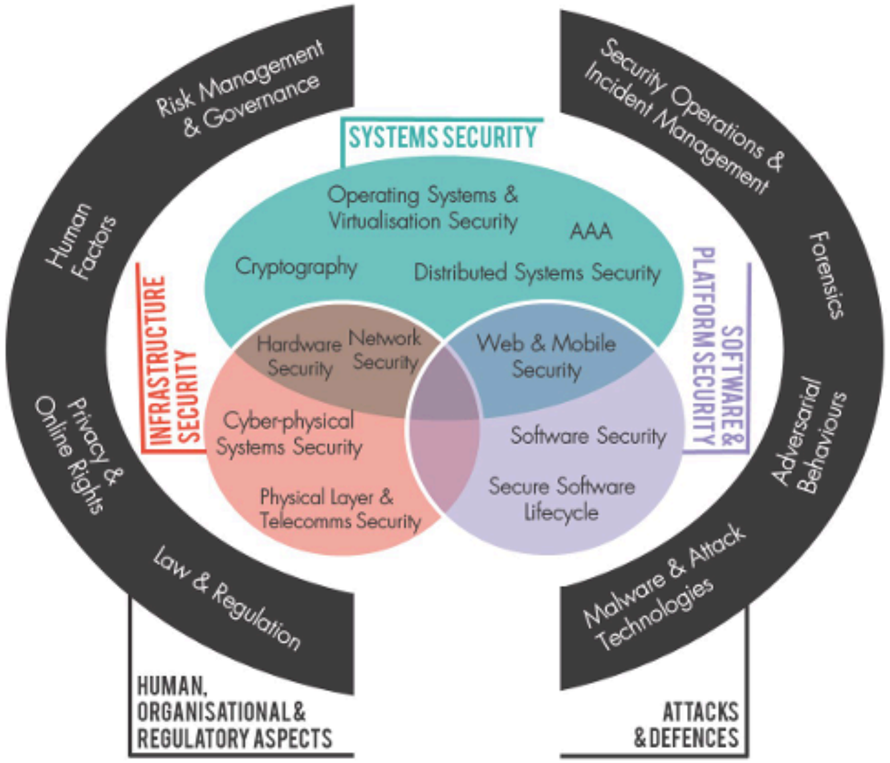
Risk Management

- Common Issues
- Risk Management Process
- Risk Frameworks

Recap

There are five major knowledge areas within cybersecurity which include:

- Attacks and Defenses
- **Human, Organizational and Regulatory aspects**
- Infrastructure Security
- System Security
- Software and Platform Security



Source: CYBOK

01
Human Factors

Objectives

Hacktales

01

Discuss common errors that are inherently human.

02

Evaluate the impact of human error on organizations.

03

Investigate strategies to minimize human error.

Hacktales

According to IBM, **95%** of cyber security breaches are primarily caused by human error.

Hacktales

Human Error Threats

1. Weak passwords
2. Careless handling of data
3. Inadequate software security
4. Low security awareness
5. Inadequate data access management

Hacktales

Psychology of Human Error

Source: Tessian Research

Module 4: Risk Management
Cybersecurity Foundation Program

Date:
May 17, 2025

Human Factor Strategies

Hacktales

Leadership Engagement

Awareness & Training

02
Cybersecurity Governance

Objectives

Hacktales

01

Understand the importance of Governanace.

02

Evaluate global cybersecurity laws and regulations.

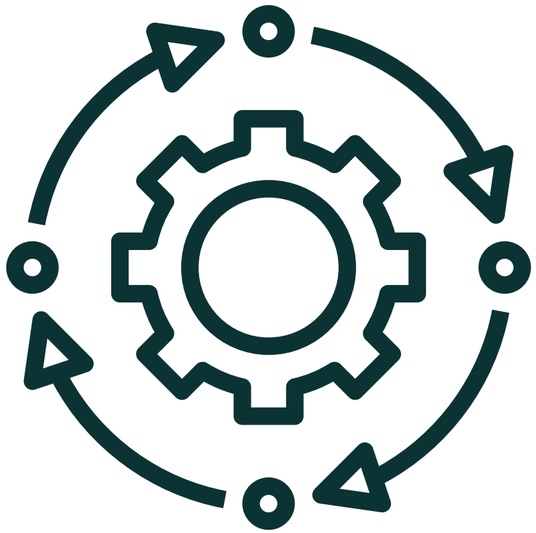
03

Review cybersecurity policies in line with industry standards.

What is Governance?

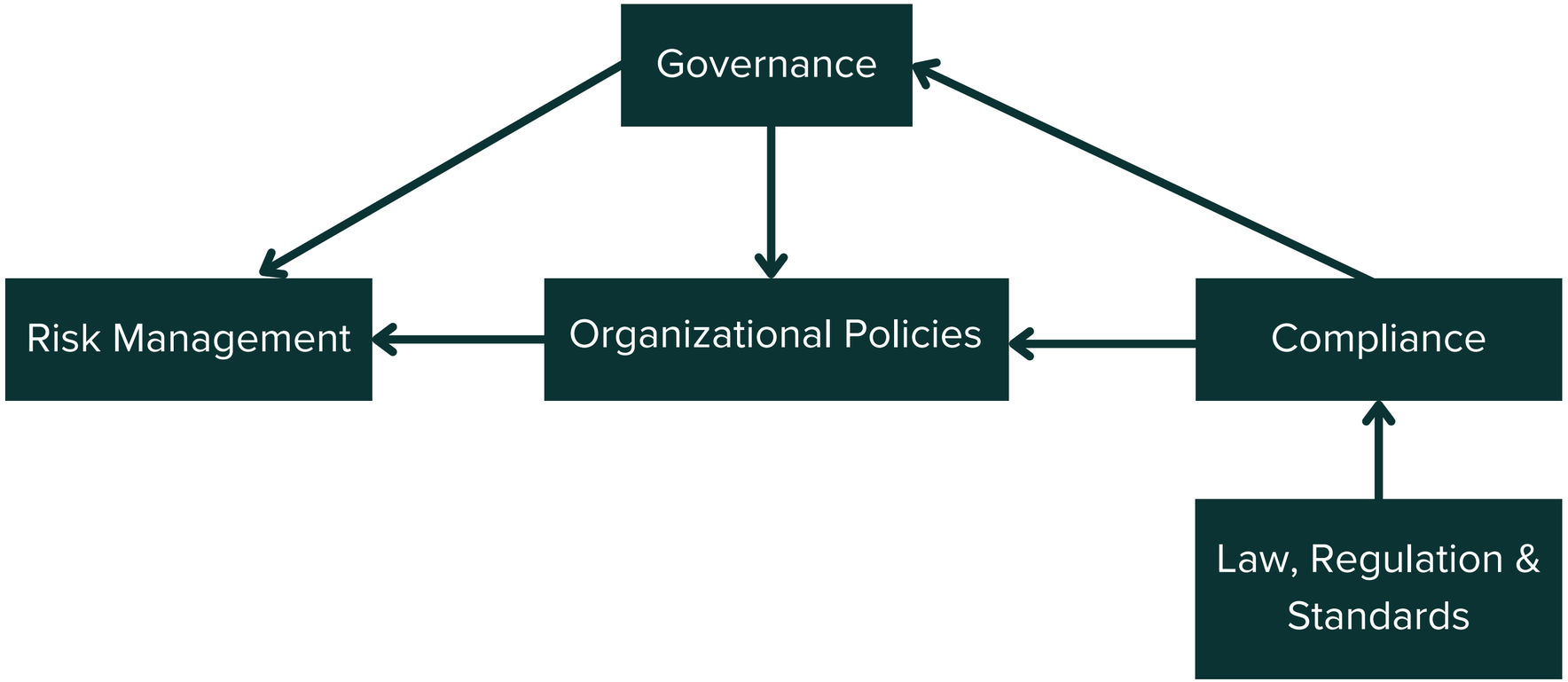
Hacktales

An architecture that ensures a company's security programs align with business objectives, comply with regulations and standards and achieves objectives for managing risk.



Governance Structure

Hacktales



Compliance

Hacktales

Cybersecurity compliance means adhering to standards and regulatory requirements that apply to an industry.

The focus is the protection of sensitive data such as:

- Personally identifiable information (PII)
- Protected health information (PHI)
- Payment card industry (PCI)

Law, Regulations and Standards

Hacktales

- **Cyber Law** is the part of the overall legal system that deals with the internet, cyberspace, and their respective legal issues e.g. **Data Protection**.

- **Regulations** are enacted by government agencies to specify the implementation of a law e.g. **General Data Protection Regulation (GDPR)**.

- Regulations incorporate **Standards** — best practices that have been assembled and vetted by a trusted organization. **(PCI-DSS, NIST, ISO 27001)**

Hacktales

Organizational Policy

A security policy is a high-level document or set of documents that describe in detail, the security controls to implement in order to protect an organization from threats.

Hacktales

Types of Security Policy

I. PROMISCIOUS

This policy does not impose any restrictions on the usage of system resources. *E.g A public library's Wi-Fi network.*

II. PERMISSIVE

With a permissive policy, only known dangerous services, attacks or behaviors are blocked. *E.g A university's network for students.*

III. PRUDENT

A prudent policy starts with all the services blocked. The administrator then permits safe and necessary services. *E.g A corporate office network.*

IV. PARANOID

This policy forbids everything. There’s a strict restriction on all use of IT resources within the organization. *E.g A financial institution's secure network for handling high-value transactions.*

Hacktales

Policy Workshop

- NIST Policy Template Guide

Module 4: Risk Management
Cybersecurity Foundation Program

03
Risk Management

Objectives

Hacktales

01

Learn the attributes of an ineffective risk management program.

02

Evaluate the six steps involved in a standard risk management process.

03

Understand the importance of risk management within an organization.

Hacktales

Why do we manage risk?

Cyber threats are constantly evolving.

The most effective way to protect your organisation against cyber attacks is to adopt a risk-based approach to cyber security.

Hacktales

Common Risk Issues

1. Poor articulation of risk scenarios
2. Compliance-oriented approach
3. Absence of risk tolerance
4. Determining risk likelihood based on the past
5. Treating risks with poor controls

Hacktales

What is Risk Management?

The process of identifying, analyzing, evaluating and mitigating an organization's cyber security threats.

Module 4: Risk Management
Cybersecurity Foundation Program

Date:
May 17, 2025

Establish Context

Hacktales

Establishing the context defines the scope for the risk management process and sets the criteria against which the risks will be assessed.

1. Define Risk
2. Determine Risk Tolerance
3. Define Roles and Responsibilties

Define Risk

Hacktales

Risk = Function (**Likelihood**, **Impact**)

Risk is defined as a function of:

- The likelihood of a given threat event exercising on a vulnerability of an asset.
- The resulting impact of the occurrence of the threat event.

Hacktales

Risk Tolerance

The level of risk acceptable to achieve a specific business objective.

Determining risk tolerance allows the management to articulate how much risk the organisation is willing to accept.

Risk Level	Risk Tolerance Description
Very High	This level of risk cannot be accepted and would create an impact so severe that the related activity would need to cease immediately. Alternatively, mitigation or transference strategies need to be taken immediately.
High	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 1 month.
Medium High	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 3-6 months.
Medium	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be regularly monitored to ensure that any change in circumstance is detected and acted upon appropriately.
Low	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be periodically monitored to ensure that any change in circumstances is detected and acted upon appropriately.

Roles and Responsibilities

Hacktales

1. Head of Organization
2. Business Owner | Unit Head
3. Risk Management Function

Business Function

4. Technology & Operations Function
5. Cybersecurity Function

Technical Function

Hacktales

Risk Assessment

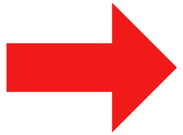
Risk assessment is about identifying risks that are specific to the environment, analyzing such risks and evaluating the risk level.

Risk Identification

Hacktales

Task 1: Identify Assets

Identify and create an inventory of all physical and logical assets that make up the system that is within the risk assessment scope.



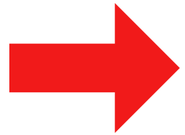
1. Crown Jewels
2. Stepping Stones

Risk Identification

Hacktales

Task 2: Identify Threats

Identify the threat events that could exploit the vulnerabilities for each identified asset.



Review publicly available sources with threat libraries for identifying threats.

Risk Identification

Hacktales

Task 3: Construct Risk Scenarios

Develop “what could go wrong” scenarios that provide realistic and relatable view of risks based on the business context, system environment and pertinent threats.

Legend: Threat Event | Vulnerability | Asset | Consequence

Attacker performs an SQL injection on an **unpatched legacy web application** to **download sensitive patient medical records**.

***Example 1**: Risk Scenario*

Internal staff makes a fraudulent payment instruction exceeding bank account balance on the **payment system** with **no set limit**, **resulting in a bank overdraft**.

***Example 2**: Risk Scenario*

Unauthorised employee accesses the **SCADA server** using **default login credentials** and **execute shutdown command** to **disrupt the water supply to the entire east side of Singapore**.

***Example 3**: Risk Scenario*

Attacker delivers spear-phishing email to **unsuspecting user**, which when clicked, triggers the **user account** to **perform SMB authentication with malicious server** and **discloses hashed credentials**.

***Example 4**: Risk Scenario*

Risk Analysis

Hacktales

Task 1: Determine Likelihood

The likelihood of cybersecurity risks should be assessed from the perspective of threats and vulnerabilities.

1. **Discoverability**
2. **Exploitability**
3. **Reproducibility**

Risk Analysis

Hacktales

- Assign a score for each of the 3 likelihood factors (i.e. 1 – 5).
- Average the score and round off to the nearest whole number.
- The final score will be the likelihood of the risk scenario; 5 being “Highly Likely” and 1 being “Rare”.

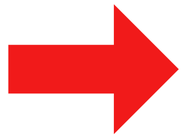
Likelihood Rating	Discoverability	Exploitability	Reproducibility
Highly Likely (5)	The vulnerability of the target: • can be discovered by searching / scanning the public domain for published information (e.g. Shodan, ExploitDB); • can be discovered and attacked from external networks (including the internet)	The attack: • can be performed with no access rights of the target; • can be performed with publicly available tools without technical knowledge	The attack: • can be repeated at will without any specific configuration[10] or event condition[11] • can be repeated at will without any customisation of the published exploits
Likely (4)	The vulnerability of the target: • can be discovered by probing the target (e.g. port scans); • can be discovered and attacked from adjacent subnets or network segments	The attack: • can be performed with restricted access rights of the target (e.g. user); • can be performed with publicly available tools with basic technical knowledge	The attack: • can be repeated given certain configuration in the target • can be repeated with minimal customisation of the published exploits (e.g. change of parameters)

Risk Analysis

Hacktales

Task 2: Determine Impact

The manifestation of a risk scenario can compromise the security of assets across three levels.



1. National
2. Organizational
3. Individual

Risk Analysis

Hacktales

- Determining the risk impact on a rating scale of 1 to 5 (5 being “Very Severe” and 1 being “Negligible”).

Impact Rating	Confidentiality	Integrity	Availability
Very Severe (5)	The unauthorised disclosure of information could be expected to have an exceptionally grave adverse effect on organisation, individuals, or the nation	The unauthorised modification or destruction of information could be expected to have an exceptionally grave adverse effect on organisation, individuals, or the nation	The disruption of access to or use of information or computer system could be expected to have an exceptionally grave adverse effect on organisation, individuals, or the nation
Severe (4)	The unauthorised disclosure of information could be expected to have a serious adverse effect on organisation, individuals, or the nation	The unauthorised modification or destruction of information could be expected to have a serious adverse effect on organisation, individuals, or the nation	The disruption of access to or use of information or computer system could be expected to have a serious adverse effect on organisation, individuals, or the nation

Risk Evaluation and Prioritization

Hacktales

Task 1: Evaluate and Prioritize Risk

This can be diagrammatically presented using a risk matrix.

IMPACT	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Highly Likely (5)
Very Severe (5)	Medium (5)	Medium High (10)	High (15)	Very High (20)	Very High (25)
Severe (4)	Low (4)	Medium (8)	Medium High (12)	High (16)	Very High (20)
Moderate (3)	Low (3)	Medium (6)	Medium (9)	Medium High (12)	High (15)
Minor (2)	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium High (10)
Negligible (1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)

LIKELIHOOD

Risk Treatment

Hacktales

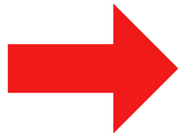
Task 1: Document and Treat Risk

A risk management process is incomplete without documentation. The outputs from previous steps must be clearly documented in a Risk Register for communication to stakeholders.

1. Risk scenarios
2. Date Identified
3. Existing measures
4. Current risk level
5. Treatment plan
6. Progress status
7. Residual risk & Risk owner

Risk Response

Having evaluated the risks, the next step is to identify and determine the next course of action to keep the risks within the organisation’s risk tolerance level.



1. **Accept**
2. **Avoid**
3. **Transfer**
4. **Mitigate**

Risk Monitoring

Hacktales

Continuously monitor the implementation of agreed-upon risk response plans, tracking identified risks, identifying and analyzing new risks, and evaluating risk process effectiveness throughout the project.

Hacktales

Risk Management Frameworks

1. **ISO 27001:2013**
2. **NIST SP 800-53**
3. **FedRAMP**

Date:
May 17, 2025

GRC Pathways

Hacktales

1. IT Security Auditor
2. Security Awareness Trainer
3. Compliance Officer
4. Risk Analyst
5. Data Protection Officer (DPO)
6. Project Manager