Cybersecurity Audit Fundamentals

Information Security

vs

Cyber Security

What is Information Security?

Information Security refers to all physical & digital data security, practices and applications.

What is Information Security?

Information Security refers to all physical and digital data security, practices and applications.

Information

Information is processed data

What is Information Security?

Information Security refers to all physical and digital data security, practices and applications.

Information

Security

What is Information Security?

Information Security refers to all physical and digital data security, practices and applications.

Information

Security

Physical & Digital

What is Information Security?

Information Security refers to all physical and digital data security, practices and applications.

Information

Security

Physical & Digital

Practices & Applications

- Policies
- Regulations
- Procedures

- Usage
- Storage
- Destroy

What is Cybersecurity?

What is Cybersecurity?

Cyber Security

Cyber: Computer Networks – The Internet

Critical Elements of Cyber/Digital

1. Devices

Mobile Devices

Laptops

Desktops

Servers – physical & virtual

Critical Elements of Cyber /Digital

2. Network Communication

Internet

Ethernet

Bluetooth

Wired Cables

Critical Elements of Cyber/Digital

3. Systems

- Operating Systems - Windows, IOS, Linux, Android
- Application Systems – Microsoft Excel, CRM, Games, WhatsApp

Critical Elements of Cyber/Digital

4. Information

Documents

Videos

Audios

Logs

Records

Critical Elements of Cyber/Digital

Cyber

Devices → Network → Systems → Information

What is Cybersecurity?

Cyber Security

Devices → Network → Systems → Information

Protection of devices, networks, systems and information from digital attacks

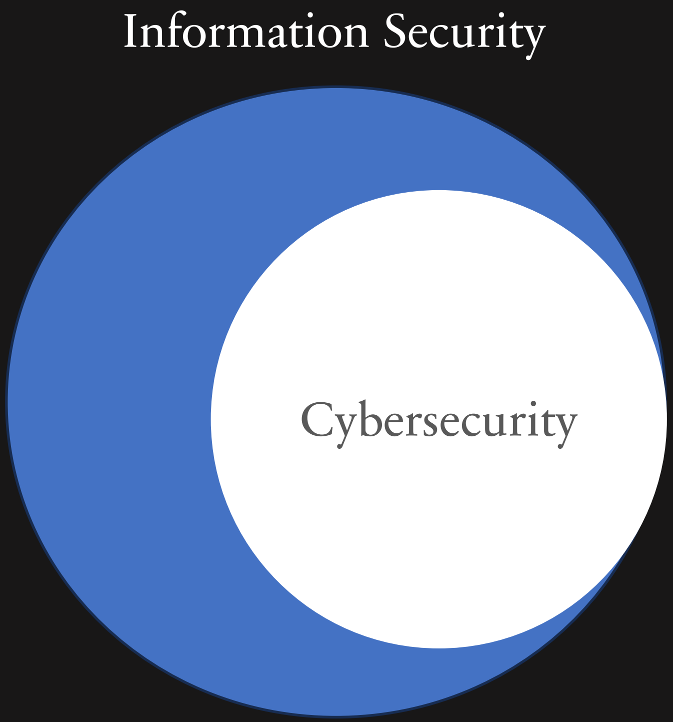
Cyber Security

vs

Information Security

Understanding Information Security

Information Security refers to all physical and digital data security, practices and applications.

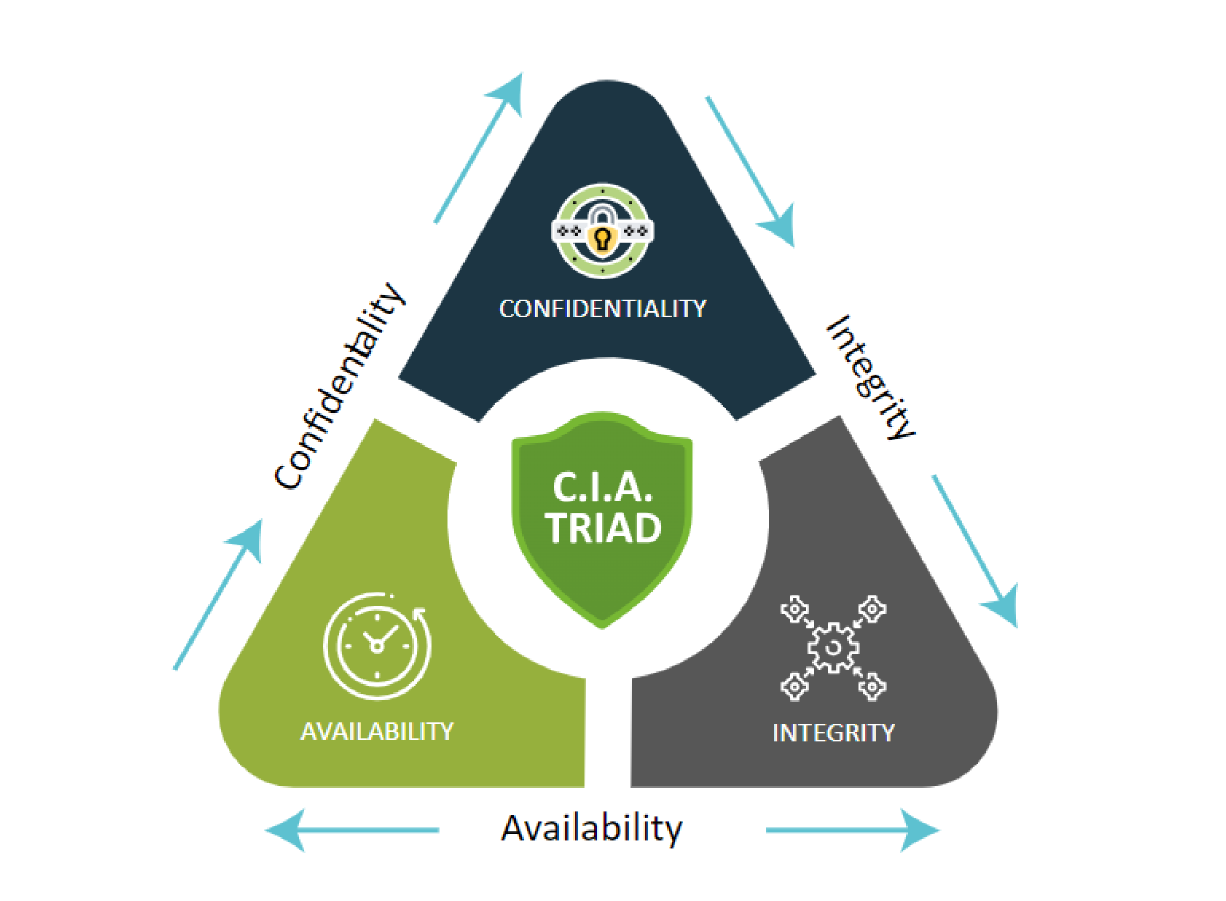


Information Security vs Cybersecurity

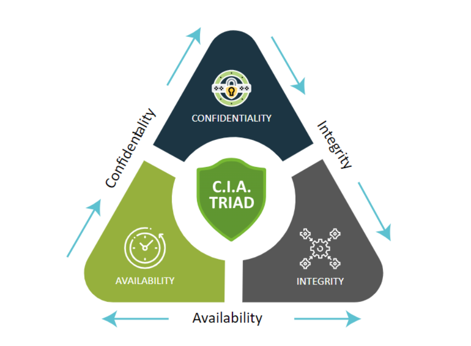
Information Security	Cybersecurity
Protecting all forms of information – digital and physical data	Protecting digital information from cyber threats – hacking, malware, phishing, ransomware
Protects the confidentiality, integrity, and availability of all types of information	Protects against unauthorized access, use, disclosure, disruption, modification, or destruction of digital information

Information Security Principle

Information Security Principle



Information Security Principle



Confidentiality

Information is only accessible to authorized persons

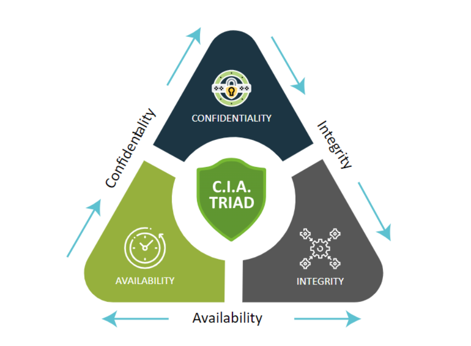
Controls:

Data Encryption

Multi-Factor Authentication

Security Tokens

Information Security Principle



Integrity

Completeness & Accuracy of Data

Controls:

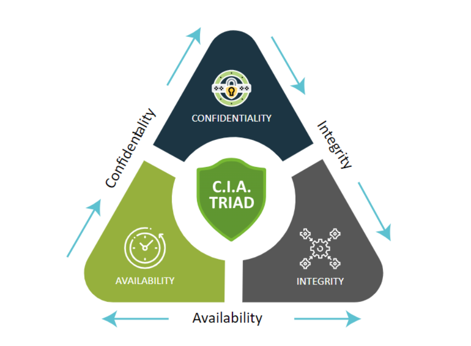
User Access Controls

Version Control

Digital Signatures

Checksums

Information Security Principle



Availability

Ability to access and use data when needed

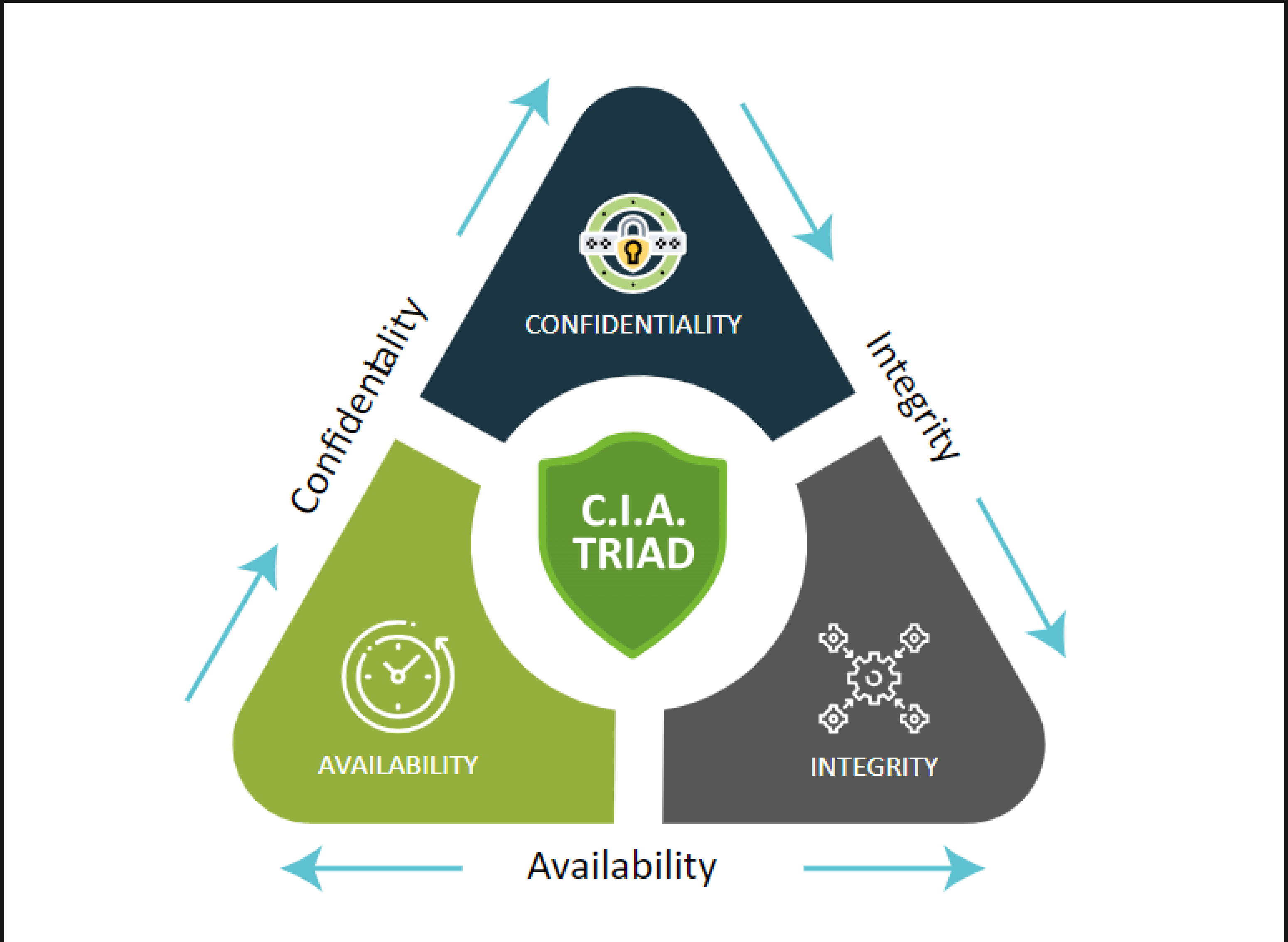
Controls:

Backup

Disaster Recovery Plan

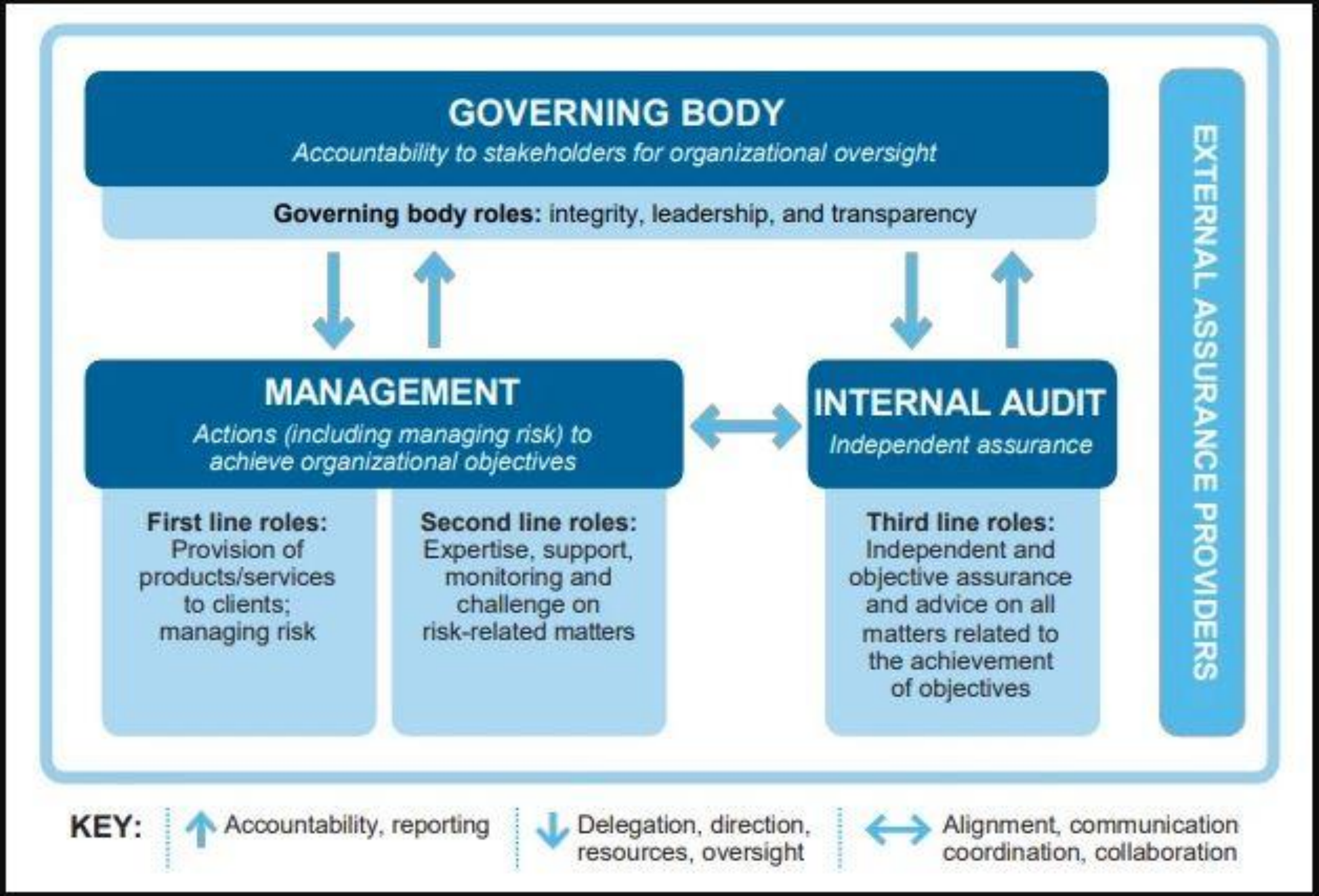
Redundancy

Information Security Principle



Cybersecurity & Organizational Structure

Three Lines of Defense Model



GOVERNING BODY

Accountability to stakeholders for organizational oversight

Governing body roles: integrity, leadership, and transparency

MANAGEMENT

Actions (including managing risk) to achieve organizational objectives

First line roles: Provision of products/services to clients; managing risk

Second line roles: Expertise, support, monitoring and challenge on risk-related matters

INTERNAL AUDIT

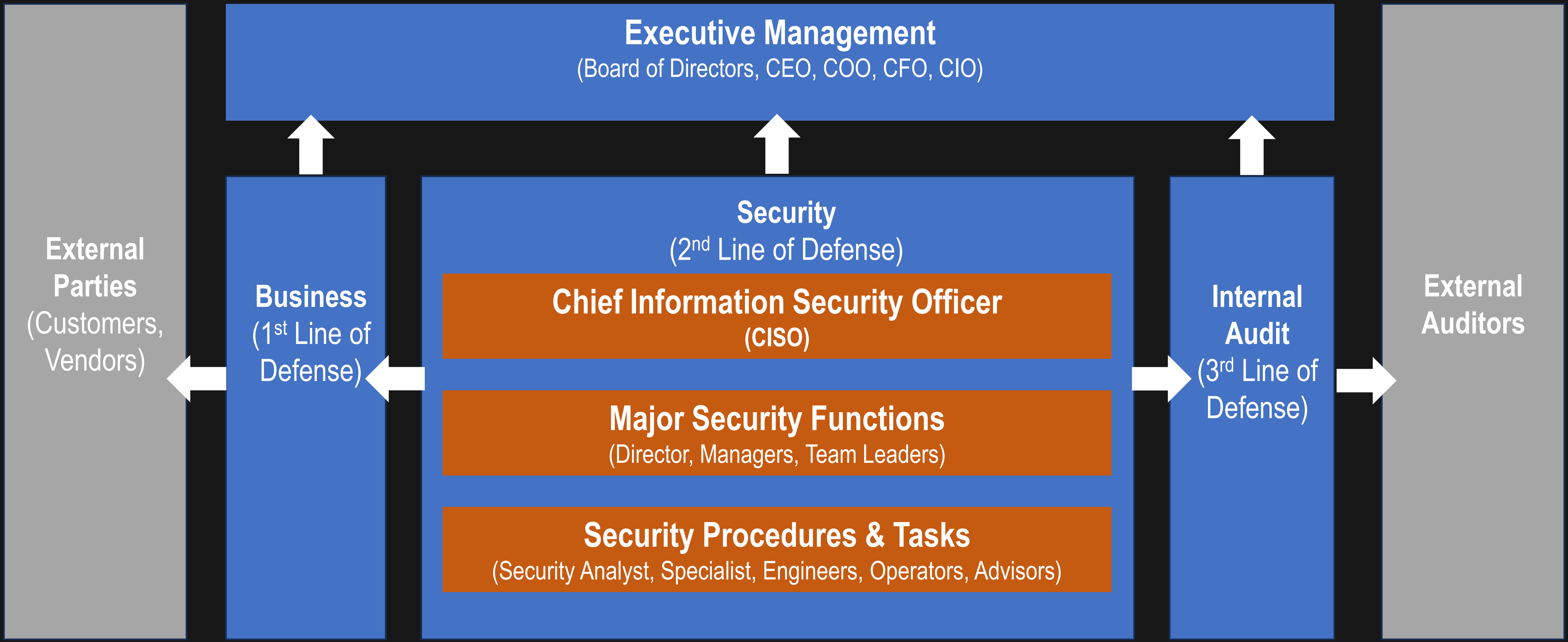
Independent assurance

Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives

EXTERNAL ASSURANCE PROVIDERS

KEY: ↑ Accountability, reporting ↓ Delegation, direction, resources, oversight ↔ Alignment, communication coordination, collaboration

Security Team Structure



Executive Management
(Board of Directors, CEO, COO, CFO, CIO)

External Parties
(Customers, Vendors)

Business
(1st Line of Defense)

Security
(2nd Line of Defense)

Chief Information Security Officer
(CISO)

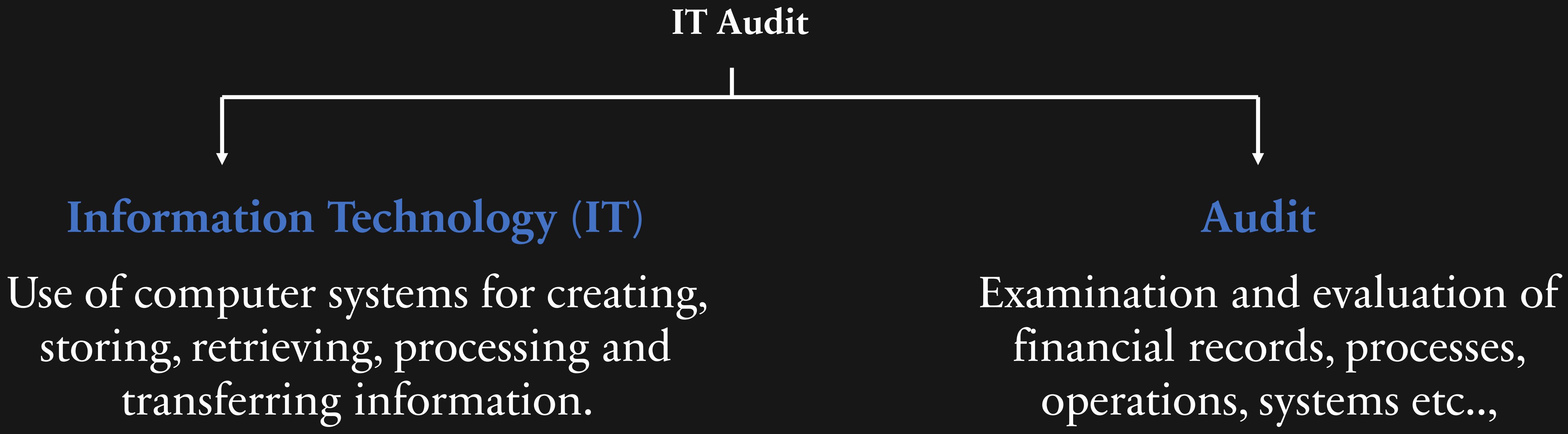
Major Security Functions
(Director, Managers, Team Leaders)

Security Procedures & Tasks
(Security Analyst, Specialist, Engineers, Operators, Advisors)

Internal Audit
(3rd Line of Defense)

External Auditors

IT Audit



IT Audit

Information Technology (IT)

Use of computer systems for creating, storing, retrieving, processing and transferring information.

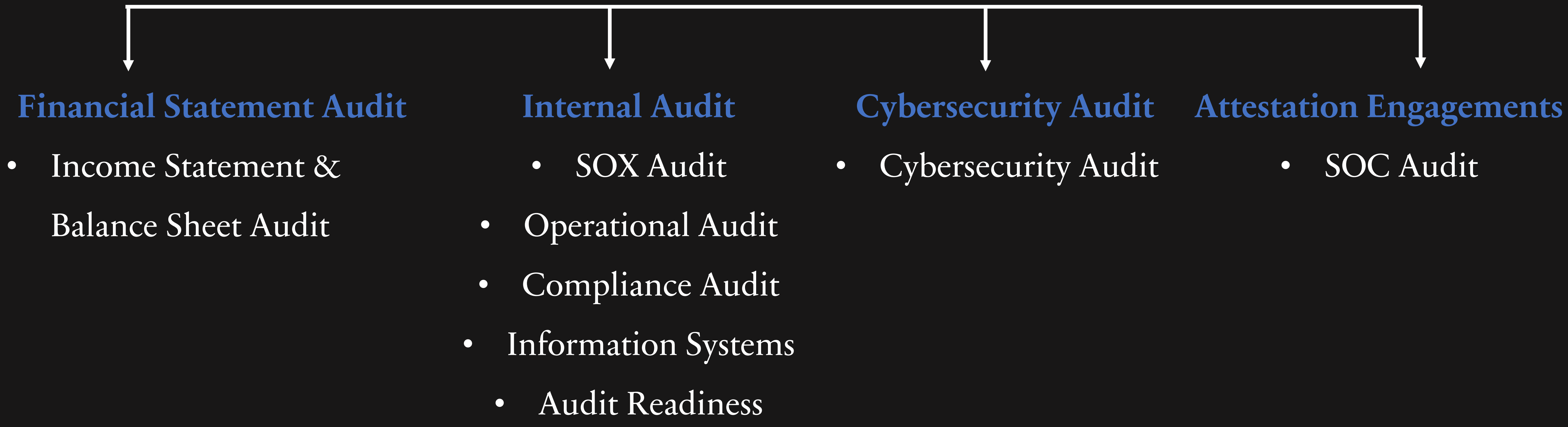
Audit

Examination and evaluation of financial records, processes, operations, systems etc..,

IT Audit is the examination and evaluation of an IT infrastructure – systems, networks, applications, data, policies and operations

Types of IT Audit

Types of IT Audit



Financial Statement Audit

- Income Statement & Balance Sheet Audit

Internal Audit

- SOX Audit
- Operational Audit
- Compliance Audit
- Information Systems
- Audit Readiness

Cybersecurity Audit

- Cybersecurity Audit

Attestation Engagements

- SOC Audit

Types of IT Audit – Financial Statement Audit

Audit Project – Income Statement & Balance Sheet

- Ensure adherence to standard accounting principles – Generally Accepted Accounting Principles (GAAP).

- Determine if the IT controls are effective & financial systems reliable for generating accurate financial reports.

- Performed by Accounting firms – Certified Public Accountants (CPA).
  - Only CPA firms are authorized to perform financial statement audit

Internal Audit Projects

1. **SOX Audit:** Assessment of Internal Controls over Financial Reporting (ICFR)in compliance with sections 302 & 404 of the SOX Act.

2. **Operational Audit:** Evaluates process changes, procedures, pricing, resource allocation and associated internal control activities

Internal Audit Projects

3. **Compliance Audit:** Adherence to laws, regulations, internal & external policies, terms of contracts

4. **Information Systems:** Information & transaction processing systems and how people use those systems.

5. **Audit Readiness:** Identify gaps in systems, internal controls, processes before an external audit

Attestation Engagement Projects

Service Organization Control (SOC) Audit:

- Attest or confirm internal controls at service organizations are in place and are properly designed and operating effectively

Internal Auditor vs External Auditor

Internal Auditor vs External Auditor

Internal Auditors are employees of the organization they audit

External Auditors are employees of a public accounting firm hired by an organization to conduct an audit

Internal Auditor vs External Auditor

Internal Auditor	External Auditor
Company employees	Outside audit firm
Hired by the company	**Appointed by shareholders' vote**
Reports are used by management	**Reports used by investors, lenders, creditors**
Conduct audit throughout the year	**Single annual audit**

Internal Audit
Roles & Responsibilities

Internal Audit Team

Internal Audit is an independent and consulting activity whose basic task is to provide assurance that the organization’s control and operations are efficient and effective.

Internal Audit Team – Roles & Responsibilities

1. **Audit Planning:** Develop or review the annual audit plan
2. **Audit Execution:** Conduct various types of audit
3. **Testing Controls:** Test controls that have been implemented by management

Internal Audit Team – Roles & Responsibilities

4. **Compliance Monitoring:** Ensure organization compliance with applicable laws

5. **Risk Assessment:** Identify and assess organization’s risks

5. **Communication:** Communicate findings, best practices, and recommendations

Cybersecurity Audit

Cybersecurity Audit:

- Examination and assessment of critical elements of an organization’s cyber or digital infrastructure

Devices → Network → Systems → Information

Benefit of Cybersecurity Audit

1. Identification of Vulnerabilities

Identify weaknesses and vulnerabilities in an organization’s informational asset and security protocols

Benefit of Cybersecurity Audit

2. Enhanced Protection

Insight into current security posture

Benefit of Cybersecurity Audit

3. Regulatory Compliance

Complying with industry regulations, standards & laws

Benefit of Cybersecurity Audit

4. Risk Management

Gain comprehensive view of risk landscape

Benefit of Cybersecurity Audit

5. Continuous Improvement

Continuous monitoring and improvement of security measures

Benefit of Cybersecurity Audit

6. Recommendation

Recommending specific controls or process changes

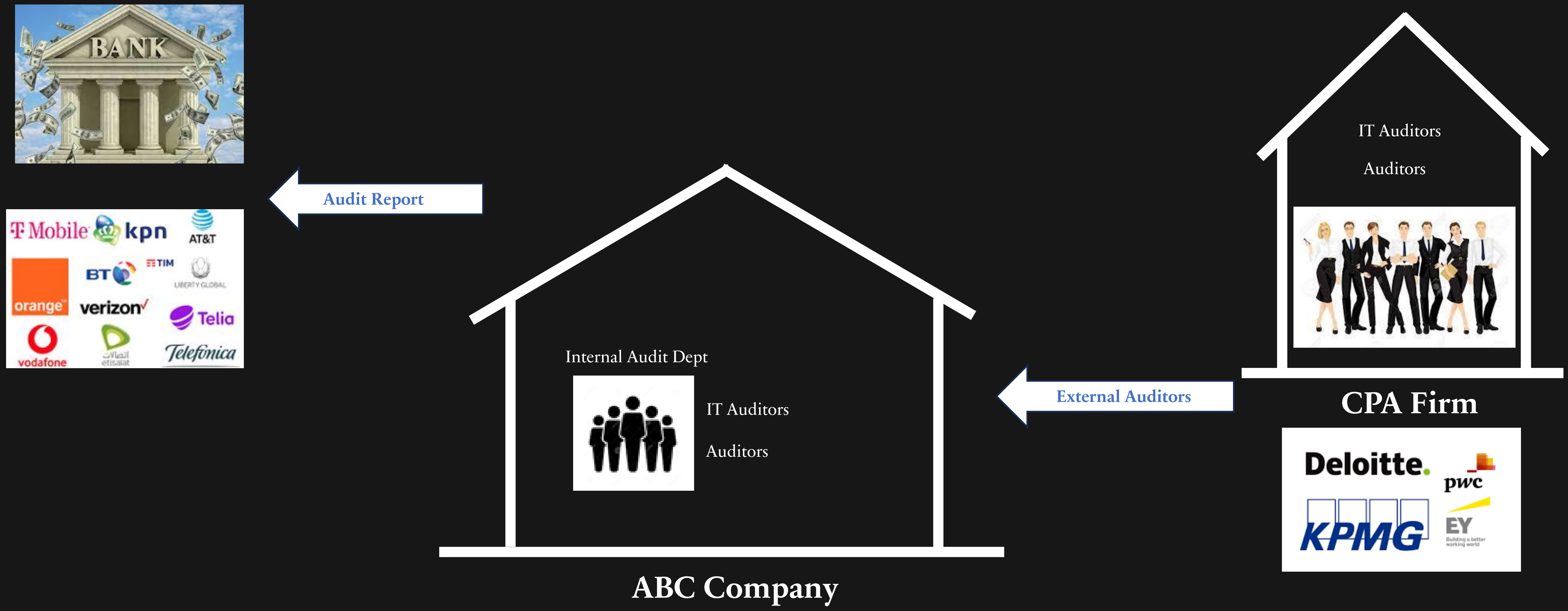
Conducting Cybersecurity Audit

Who performs a Cybersecurity Audit

1. **Internal Auditors**

2. **External Auditors**

Who performs a Cybersecurity Audit



Audit Report

Internal Audit Dept

IT Auditors

Auditors

ABC Company

External Auditors

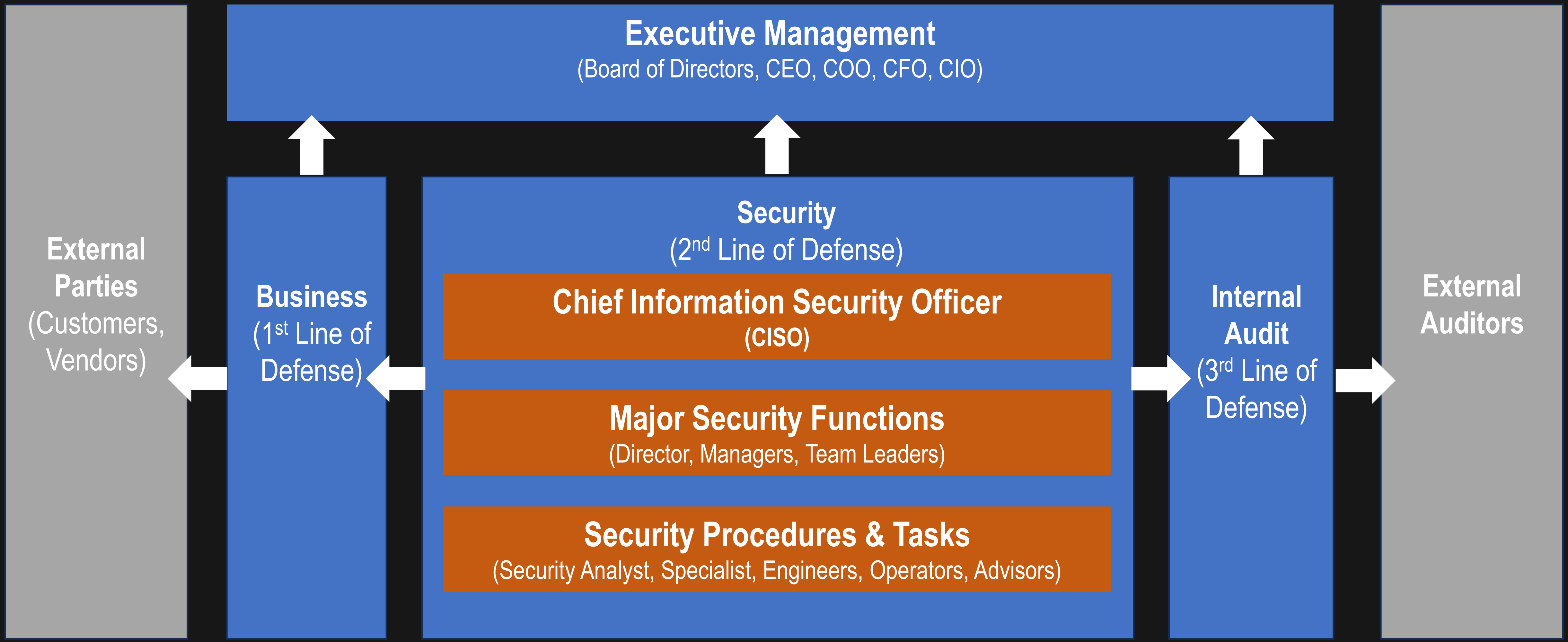
IT Auditors

Auditors

CPA Firm

IT Audit Skillset

Security Team Structure



Executive Management
(Board of Directors, CEO, COO, CFO, CIO)

External Parties
(Customers, Vendors)

Business
(1st Line of Defense)

Security
(2nd Line of Defense)

Chief Information Security Officer
(CISO)

Major Security Functions
(Director, Managers, Team Leaders)

Security Procedures & Tasks
(Security Analyst, Specialist, Engineers, Operators, Advisors)

Internal Audit
(3rd Line of Defense)

External Auditors

Controls

Controls

A control is a procedure or policy that provides a reasonable assurance that an IT environment operates as intended, that data is reliable, and that the organization comply with applicable laws and regulations.

A control is any action, policy, procedure that helps an organization mitigate risk.

Controls

Access Control

Safety Control

Input Control

Safety Control

Types of Controls

Types of Controls

- Preventive Controls
- Detective Controls
- Corrective Controls
- Deterrent Controls
- Compensating Control

Types of Controls

Preventive Control

Designed to prevent the chance of errors or fraud before occurrence

- Data Encryption
- Security Awareness Training
- Access Controls – Physical/Logical

Types of Controls

Detective Control

Designed to find errors or problems after the event has occurred.

- Log monitoring and analysis
- Vulnerability scanning
- Video surveillance

Types of Controls

Corrective/Mitigating Controls

Designed to make the system more effective to use

- Backup & recovery
- Business continuity & disaster recovery plan
- Patch management & vulnerability management

Compensating Control

Alternative measures put in place when the primary control objective cannot be met

- Manual approval process
- Temporary access restriction
- Manual data validation
- User training & monitoring

Types of Controls

Deterrent Control

These are controls used to discourage or warn against a deliberate attack

- Hardware locks
- Cable locks
- Video surveillance
- Security guards

Cybersecurity Frameworks

Cybersecurity Framework

System of standards, guidelines, and best practices to manage risks that arise in the digital world.

- Guidelines and best practices for securing Devices, Systems, Networks and Data
- Establish a culture of security, reducing risk of data breaches & cyber attacks
- Compliance with regulations and laws

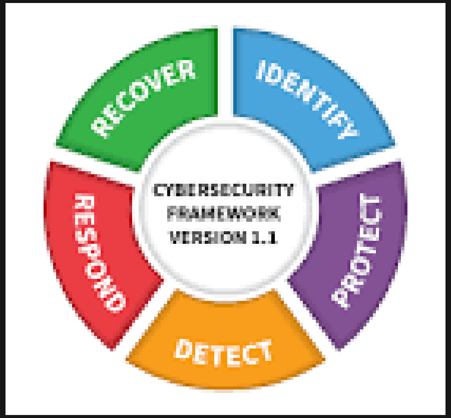
Cybersecurity Frameworks

- NIST (National Institute of Standards and Technology))
- ISO 27001 (International Organization for Standardization)
- CIS Controls (Center for Internet Security)

Compliance Frameworks

- SOC (Service Organization Control)
- GDPR (General Data Protection Regulation)
- HIPAA (Health Insurance Portability and Accountability Act)
- PCI DSS (Payment Card Industry Data Security Standard)
- COSO (Committee of Sponsoring Organization)

NIST Framework



NIST Framework – Core Functions

1. **Identify**

Determine what exists, what dangers are involved, and how it connects to the company goals

Asset Management

Risk Management

Governance

NIST Framework – Core Functions

2. Protect

Safeguarding assets and data

Access Controls

Data Encryption

Security Awareness

NIST Framework – Core Functions

3. Detect

Safeguarding assets and data

Continuous Monitoring

Incident Detection Measures

NIST Framework – Core Functions

4. Respond

Safeguarding assets and data

Notify Stakeholders

Investigate & Contain

Keep Operations Up

NIST Framework – Core Functions

5. Recover

Developing effective response strategy to mitigate impact

Repair & Restore

Communicate

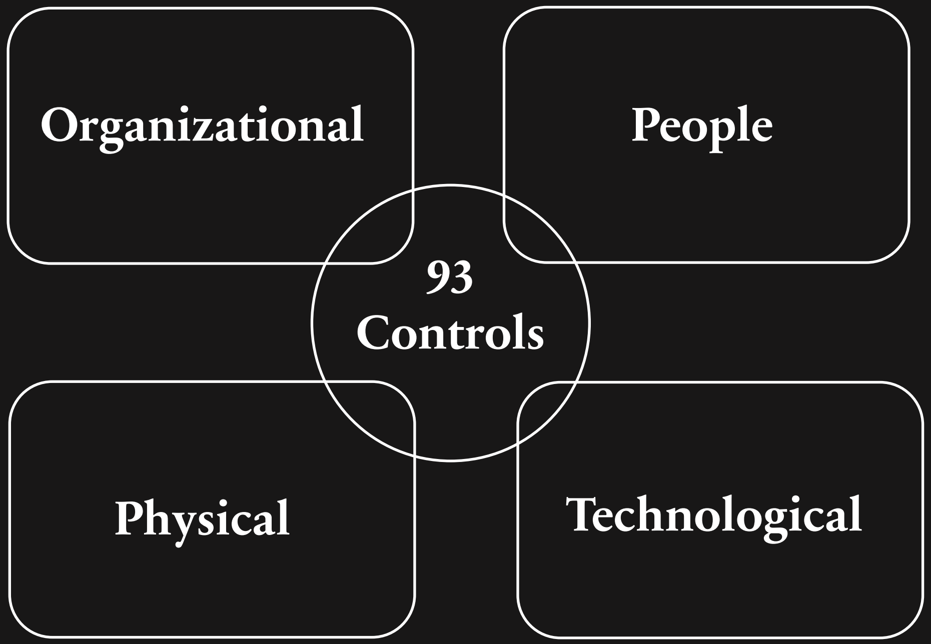
ISO 27001 Framework

ISO 27001 Framework

ISO 27001 Framework

ISO 27001 – Requirement for an ISMS

ISO 27001



Organizational

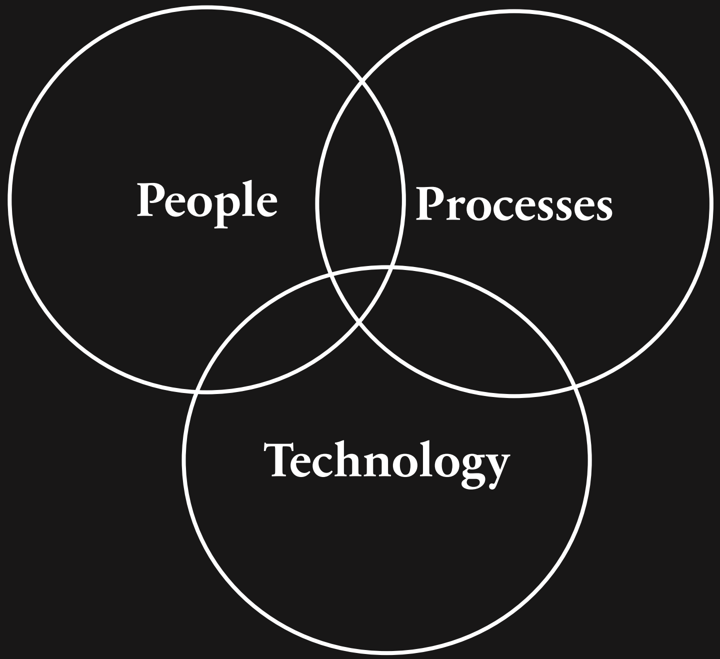
People

93 Controls

Physical

Technological

Information Security Management Systems (ISMS)



People

Processes

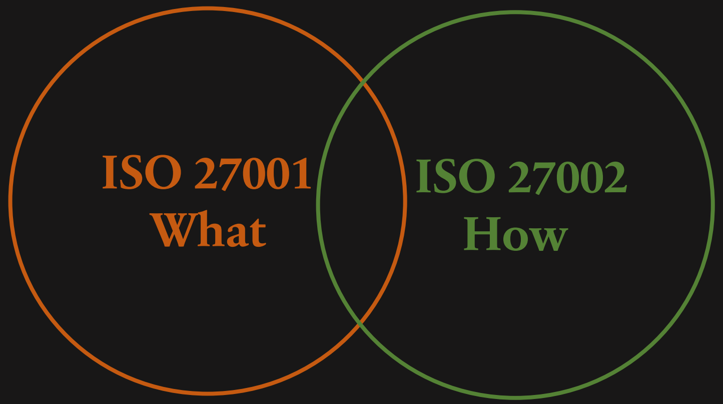
Technology

- Identify Stakeholders
- Risk Assessment
- Define Controls
- Set clear Objectives
- Implement Controls
- Continuous Measure
- Continuous Improvement

ISO Series

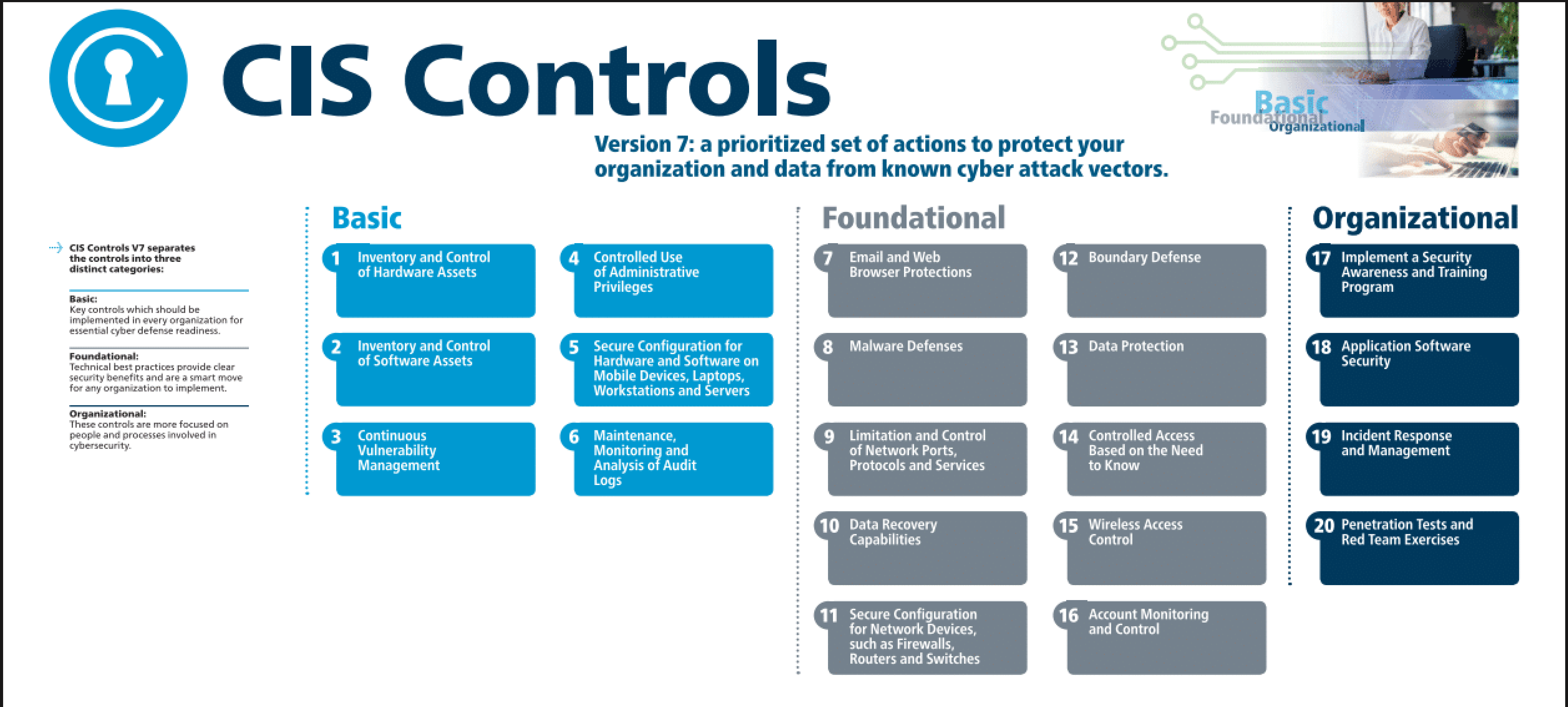
ISO 27001 – Requirement for an ISMS

ISO 27002 – Guidance on implementing Information Security Controls



CIS Framework

CIS (Center for Internet Security) Framework



CIS Controls

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.

Basic
Foundational
Organizational

CIS Controls V7 separates the controls into three distinct categories:

Basic:
Key controls which should be implemented in every organization for essential cyber defense readiness.

Foundational:
Technical best practices provide clear security benefits and are a smart move for any organization to implement.

Organizational:
These controls are more focused on people and processes involved in cybersecurity.

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

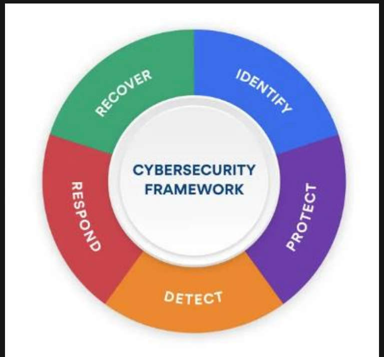
19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

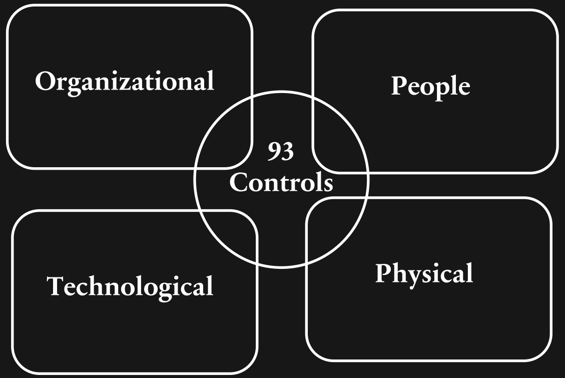
Internal Auditors & Frameworks

NIST vs ISO 27001 vs CIS

NIST 100+ Controls



ISO 27001



Organizational

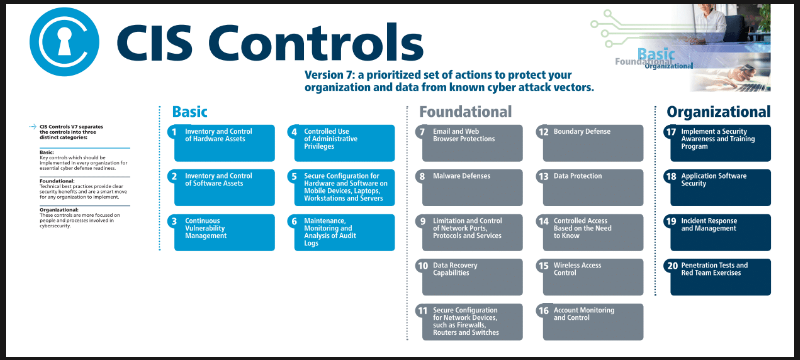
People

93 Controls

Technological

Physical

CIS Controls



CIS Controls

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.

Basic
Foundational
Organizational

CIS Controls V7 separates the controls into three distinct categories:

Basic: Key controls which should be implemented in every organization for essential cyber defense readiness.

Foundational: Technical best practices provide clear security benefits and are a smart move for any organization to implement.

Organizational: These controls are more focused on people and processes involved in cybersecurity.

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

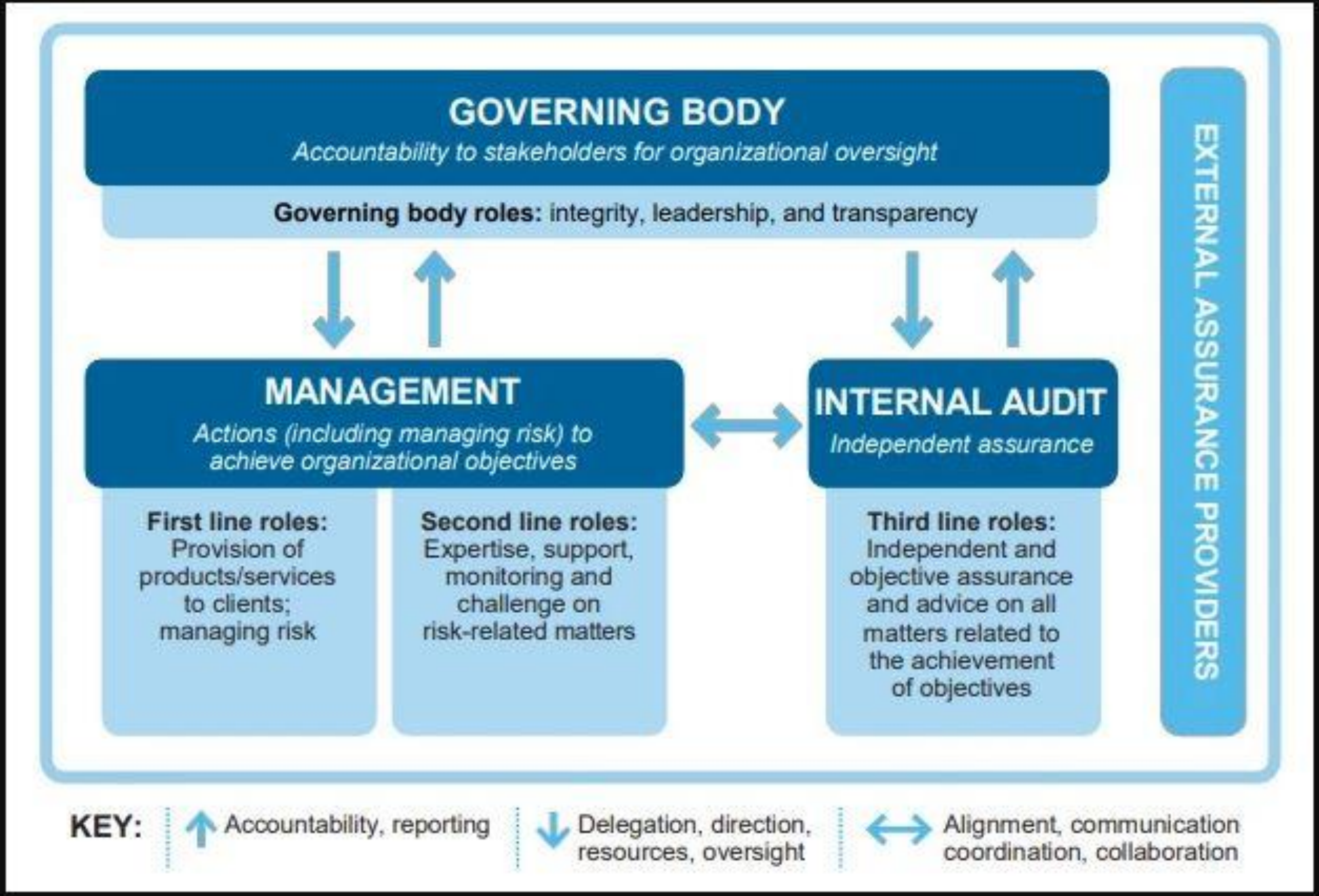
18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Implementing Frameworks

- Internal Auditors do not implement frameworks



GOVERNING BODY

Accountability to stakeholders for organizational oversight

Governing body roles: integrity, leadership, and transparency

MANAGEMENT

Actions (including managing risk) to achieve organizational objectives

First line roles: Provision of products/services to clients; managing risk

Second line roles: Expertise, support, monitoring and challenge on risk-related matters

INTERNAL AUDIT

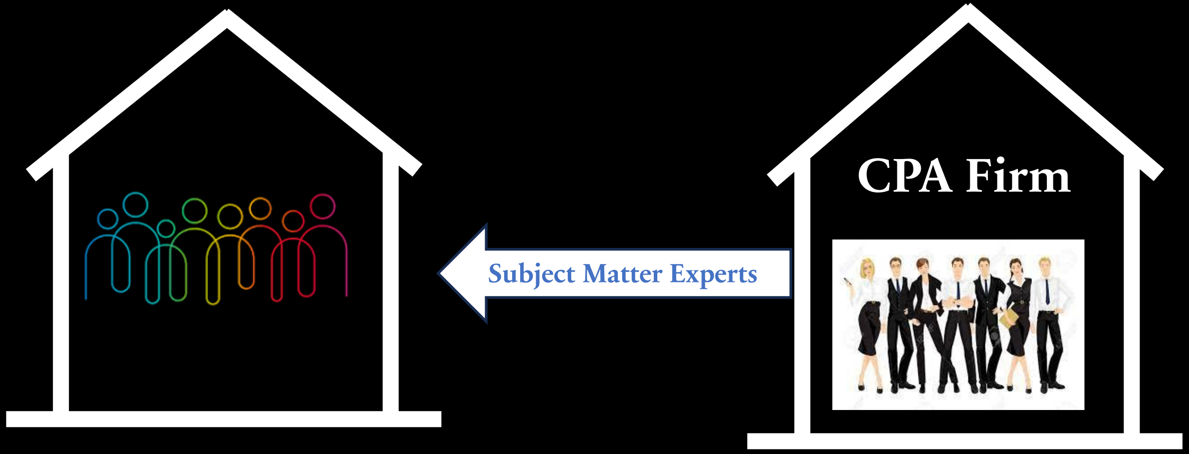
Independent assurance

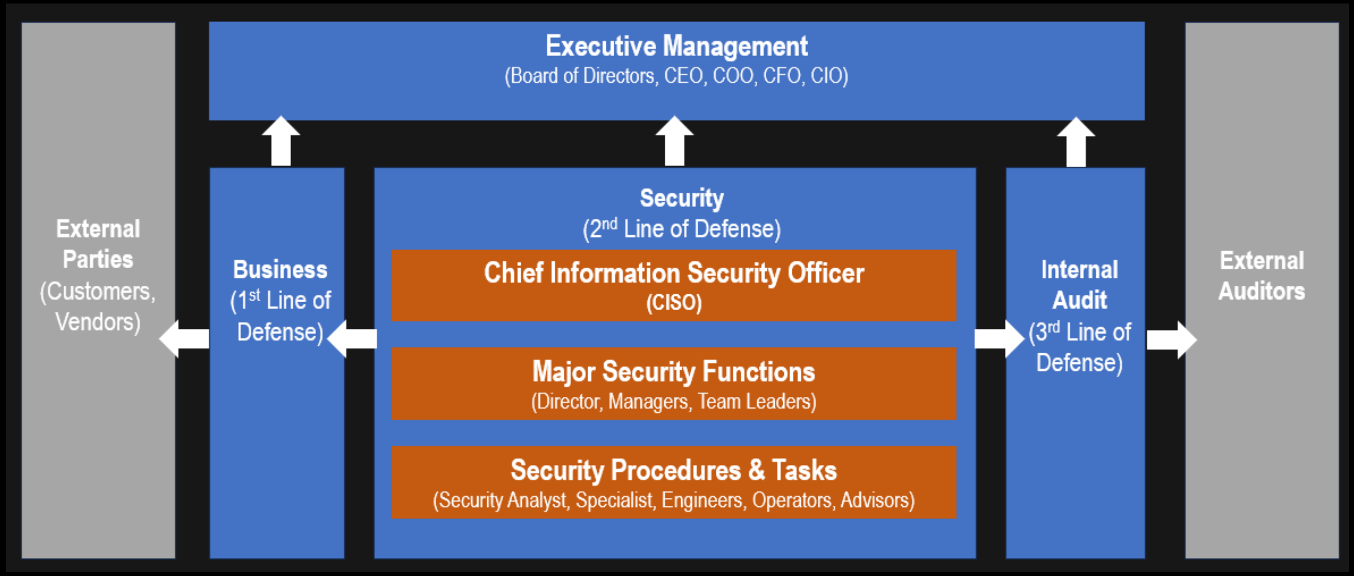
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives

EXTERNAL ASSURANCE PROVIDERS

KEY: ↑ Accountability, reporting ↓ Delegation, direction, resources, oversight ↔ Alignment, communication coordination, collaboration

IT Auditors & Frameworks





External Parties (Customers, Vendors)

Executive Management (Board of Directors, CEO, COO, CFO, CIO)

Business (1st Line of Defense)

Security (2nd Line of Defense)

Chief Information Security Officer (CISO)

Major Security Functions (Director, Managers, Team Leaders)

Security Procedures & Tasks (Security Analyst, Specialist, Engineers, Operators, Advisors)

Internal Audit (3rd Line of Defense)

External Auditors

OUR BUDGET WON'T ALLOW US TO BUY A SEGREGATION OF DUTIES SOFTWARE PACKAGE.
SO THE AUDITOR SAID WE WILL ALL HAVE TO PRESS THE ENTER KEY TOGETHER

Segregation of Duties

IT Auditors & Frameworks

- Internal Auditors do not implement frameworks or controls
- Internal Auditors test controls implemented by management
- Internal Auditors should be aware of Cybersecurity frameworks

Cybersecurity Standards

Standard vs Framework

Standards are agreed level of quality requirements. Usually well-defined and expected to be followed closely

Frameworks are broad guidelines put into practice in the absence of well-defined standards

Cybersecurity Standards

HIPAA (Health Insurance Portability and Accountability Act)

PCI DSS (Payment Card Industry Data Security Standard)

HIPAA (Health Insurance Portability and Accountability Act)

Sets standards for protecting sensitive patient healthcare information. It applies primarily to healthcare providers, health plans, and healthcare institutions.

HIPAA (Health Insurance Portability and Accountability Act)

Sets standards for protecting sensitive patient healthcare information. It applies primarily to healthcare providers, health plans, and healthcare institutions.

HIPAA – Protected Health Information (PHI)

- Name and address
- Social Security number (SSN)
- Date of birth (DOB)
- Email addresses, phone numbers, and fax no.
- Medical record numbers or account numbers

Fingerprints or facial images

Certificate/license numbers

Internet Protocol (IP) addresses

Health plan beneficiary numbers

Vehicle identifiers including license plate numbers

HIPAA Security Rule

- Administrative Safeguards: Policies, procedures and actions to protect ePHI
  - Risk assessment, training programs, incidence response

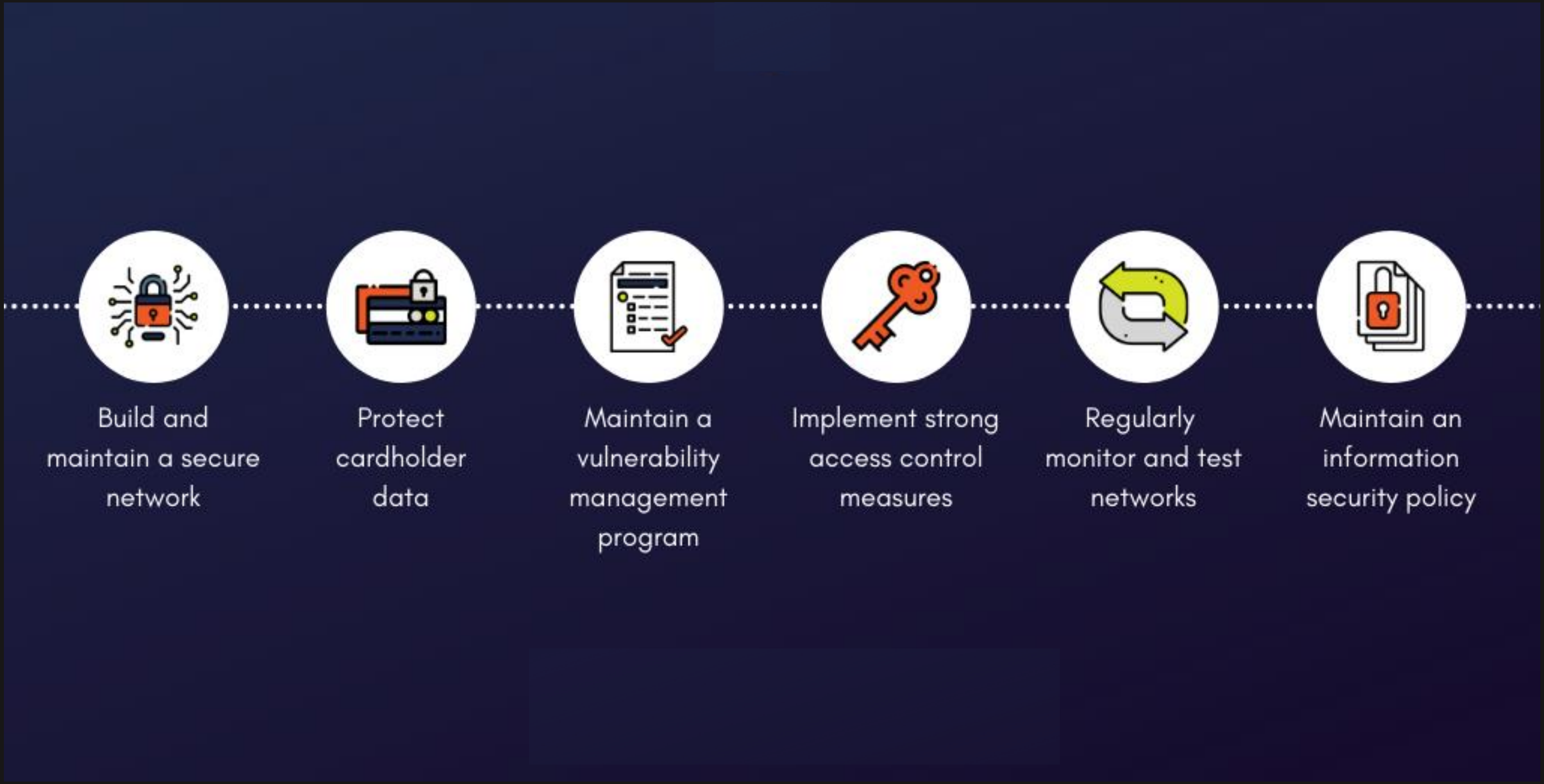
- Physical Safeguards: Physical access controls to facilities
  - Security controls, disposal policies

- Technical Safeguards: Using technology solutions such as encryption or firewalls
  - System monitoring, data integrity controls

PCI DSS (Payment Card Industry Data Security Standard)

Security standard ensuring that all companies that accept, process, store or transmit credit card information maintains a secure environment

PCI DSS Key Components



Build and maintain a secure network

Protect cardholder data

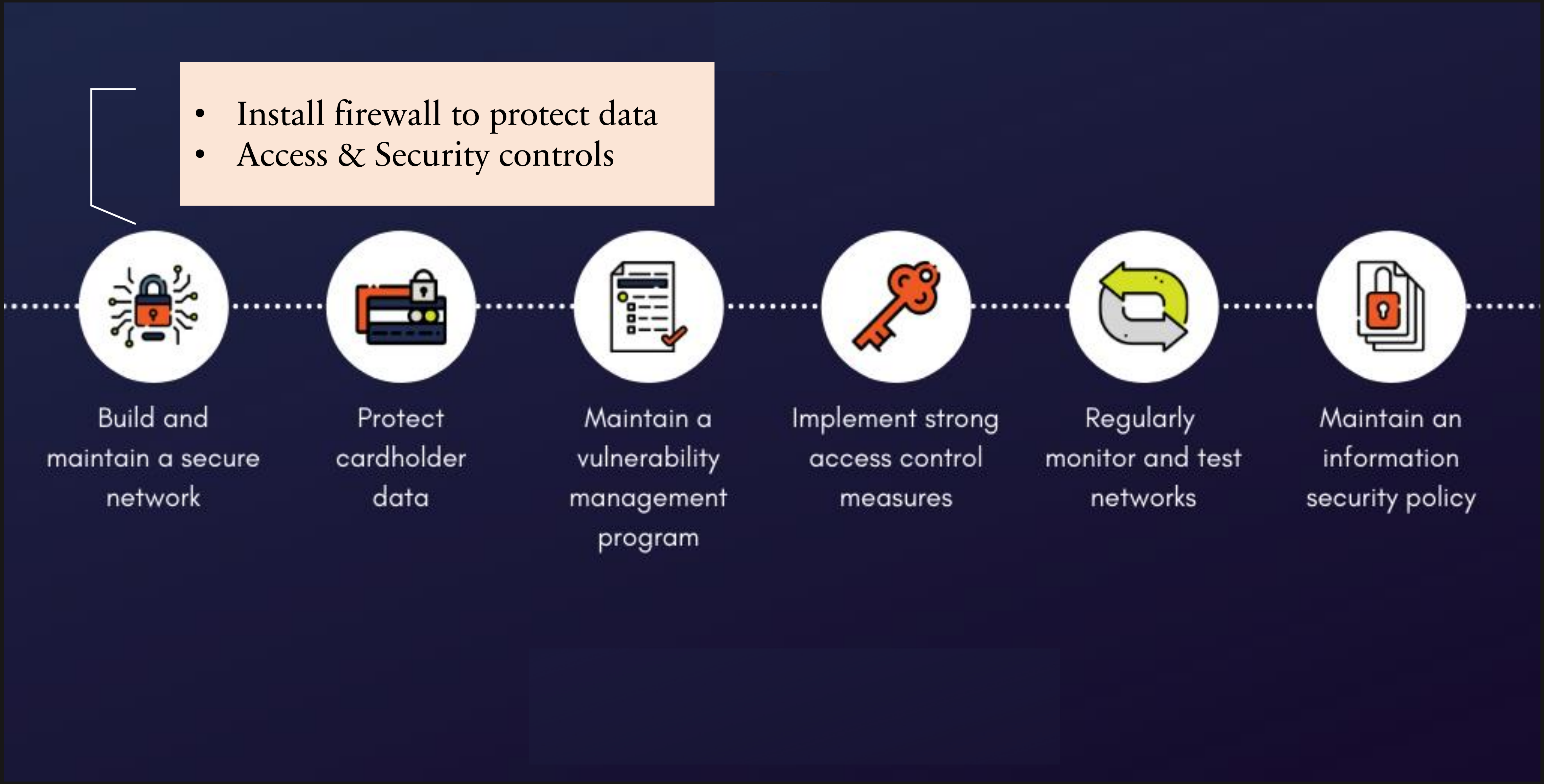
Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

PCI DSS Key Components



- Install firewall to protect data
- Access & Security controls

Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program

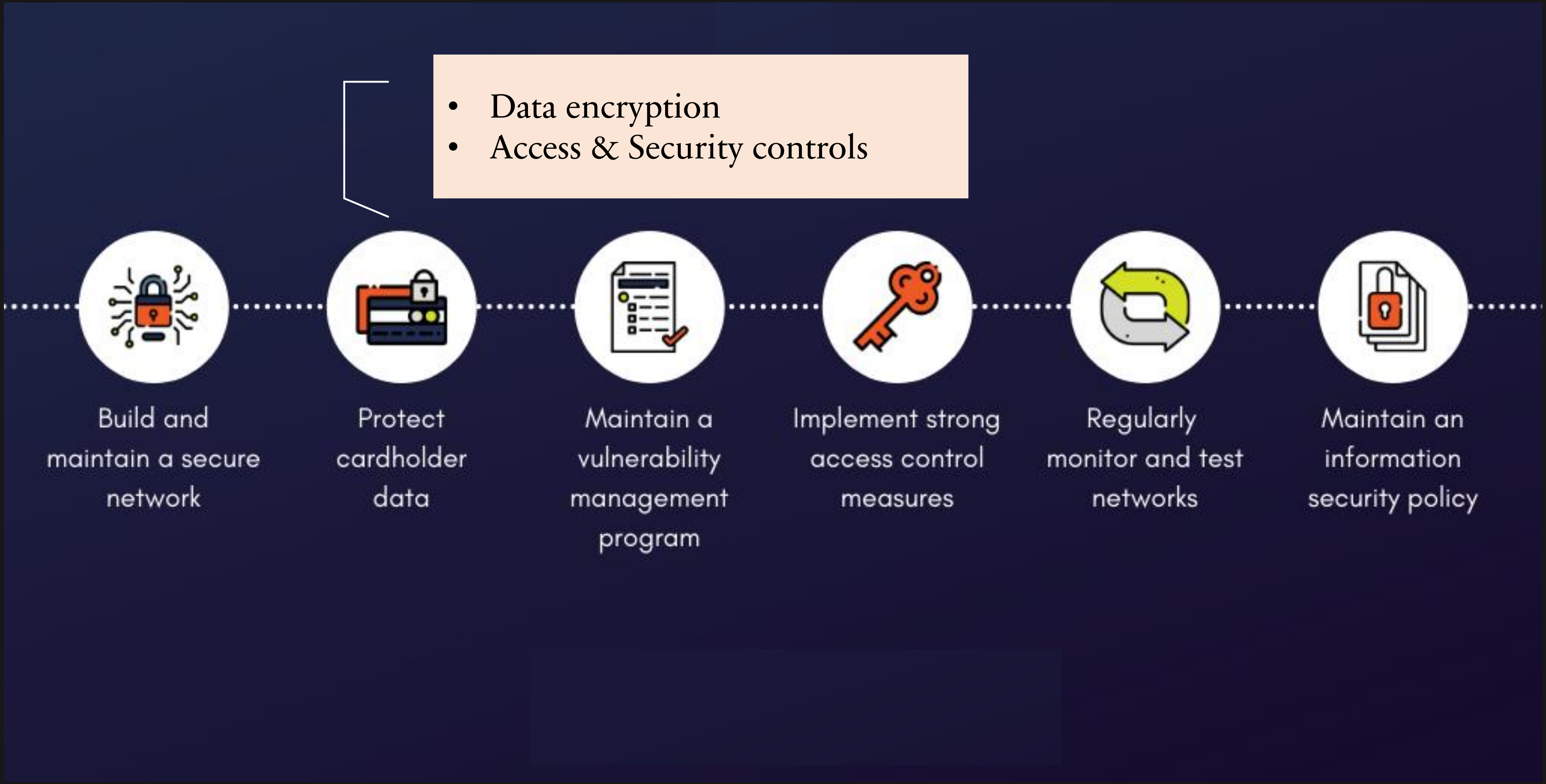
Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

PCI DSS Key Components

- Data encryption
- Access & Security controls



Build and maintain a secure network

Protect cardholder data

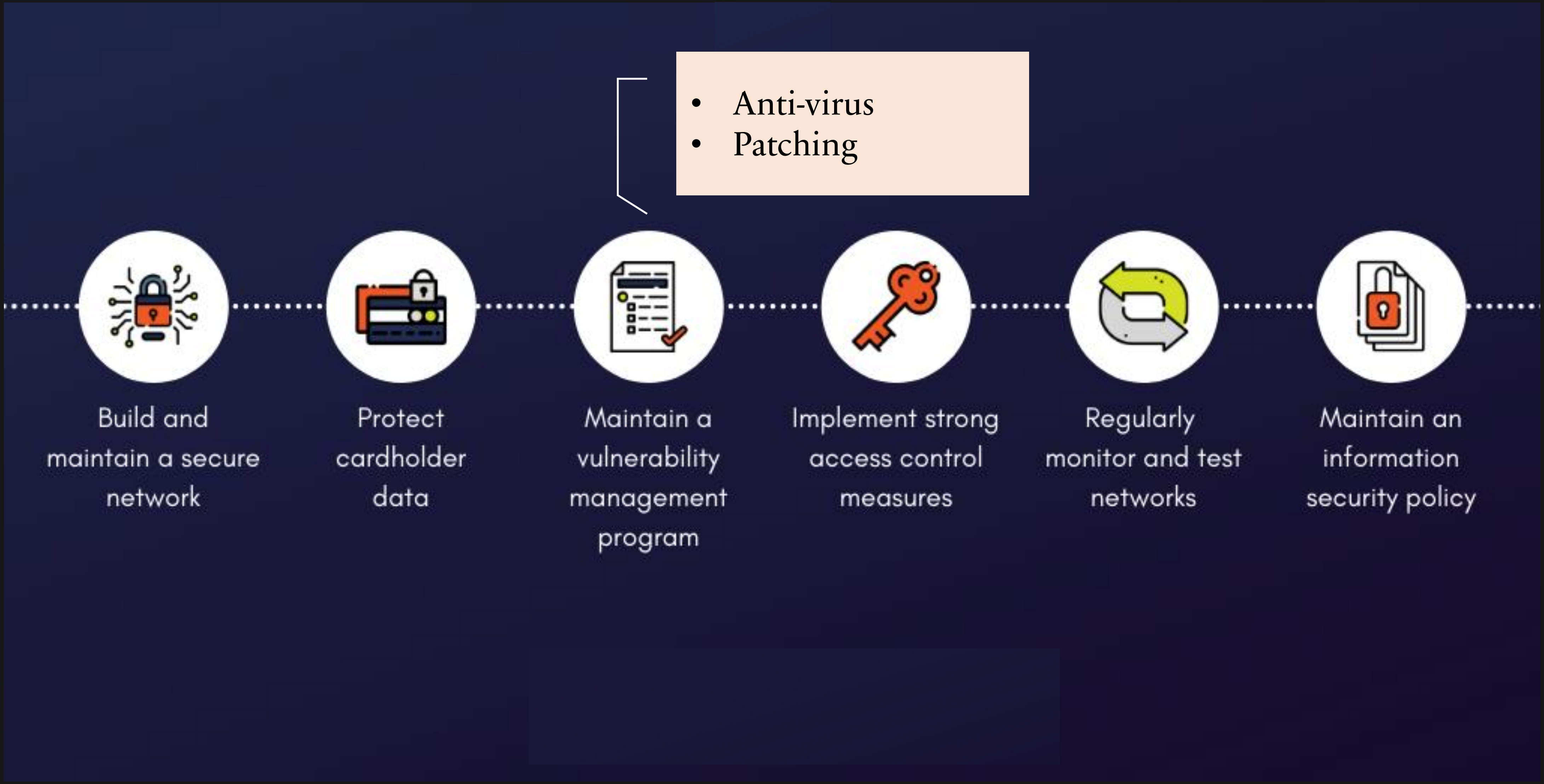
Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

PCI DSS Key Components



- Anti-virus
- Patching

Build and maintain a secure network

Protect cardholder data

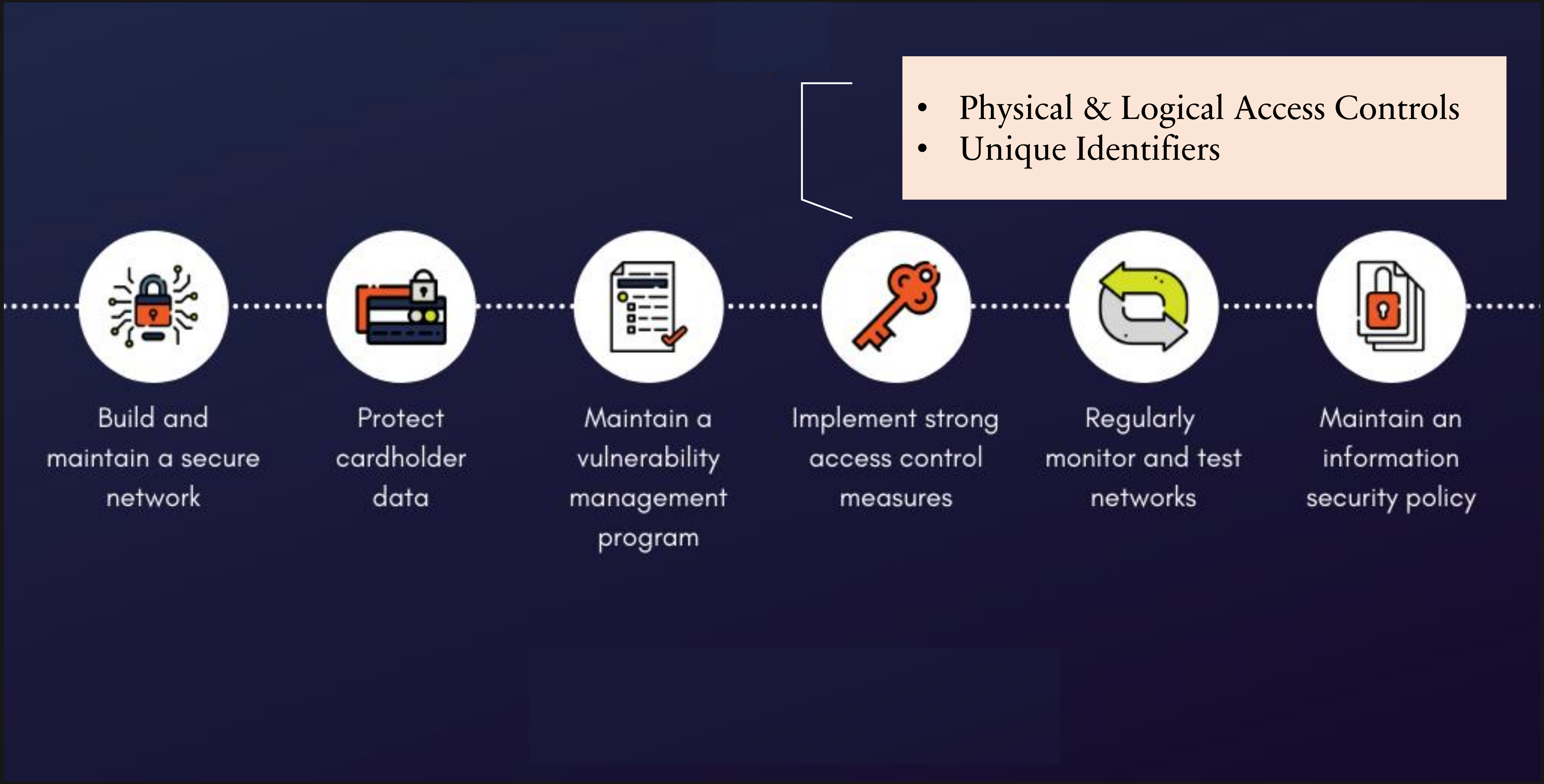
Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

PCI DSS Key Components



- Physical & Logical Access Controls
- Unique Identifiers

Build and maintain a secure network

Protect cardholder data

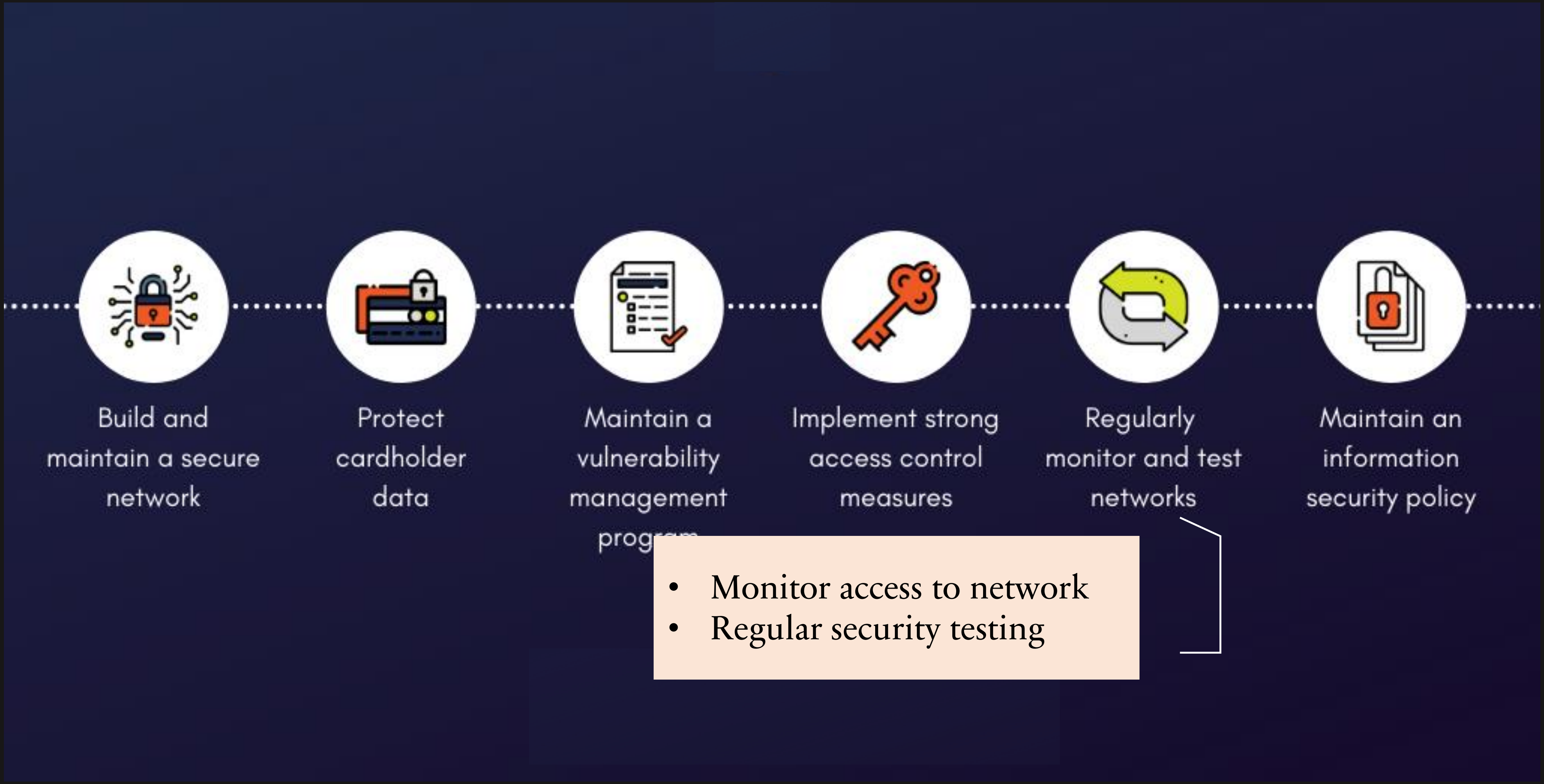
Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

PCI DSS Key Components



Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program

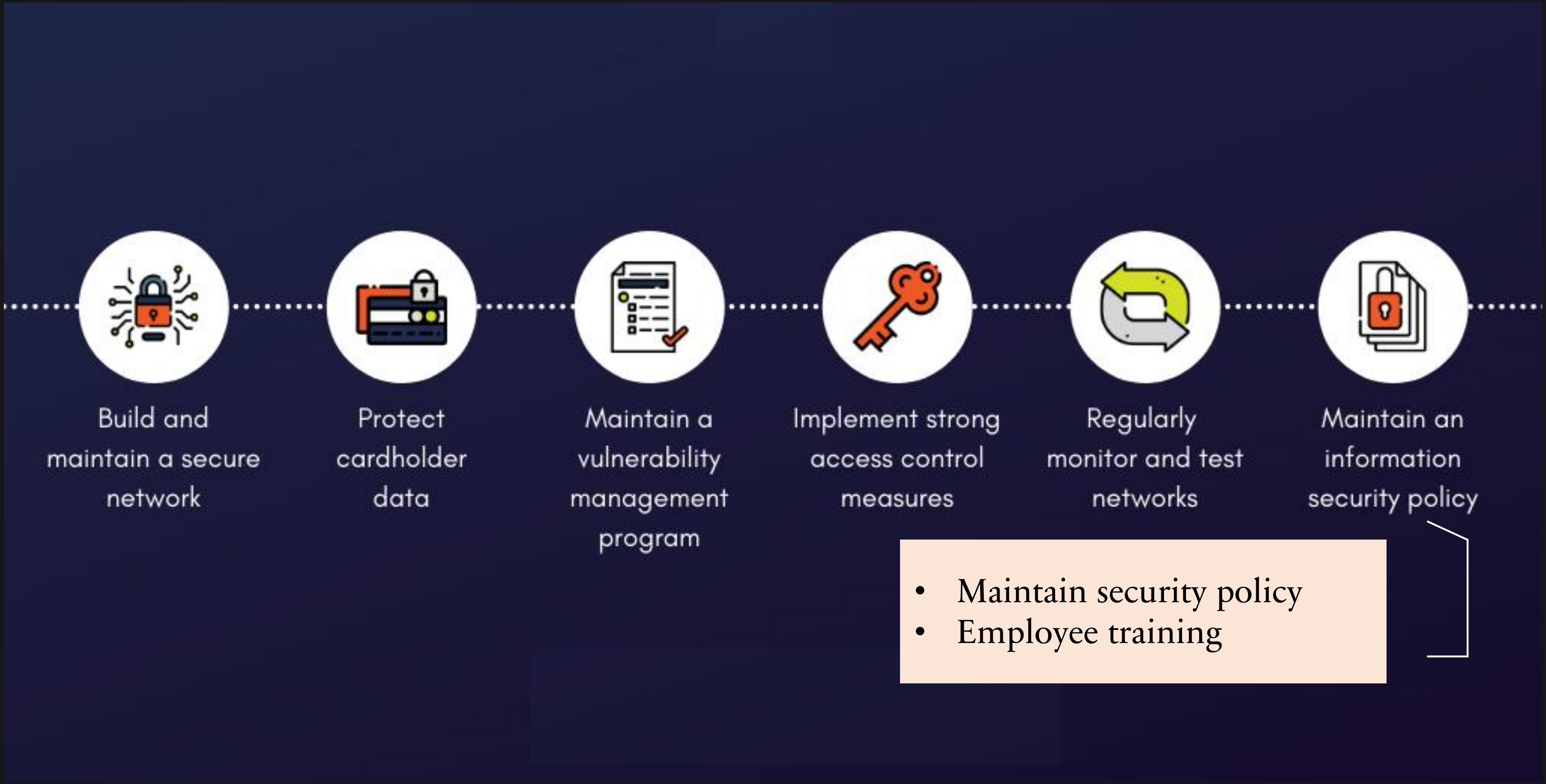
Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

- Monitor access to network
- Regular security testing

PCI DSS Key Components



- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

- Maintain security policy
- Employee training

Frameworks & Standards

Frameworks and Standards

Frameworks

- NIST
- ISO 27001
- CIS

Standards

HIPAA

PCI DSS

Implement security controls – Devices, Systems, Networks, Data

Cybersecurity Controls

Controls

A control is any action, policy, procedure that helps an organization mitigate risk.

Critical Elements of Cyber/Digital

Cyber

Devices → Network → Systems → Information

Cyber Security Controls

Safeguards to protect devices, systems, networks and data from security threats, vulnerabilities and unauthorized access

Designed to mitigate risks and ensure Confidentiality, Integrity & Availability (CIA)

Cyber Security Controls

Operational Controls

Technical Controls

Physical Controls

Operational Controls

Policies & procedures established to manage & govern security practices

- Policies and Procedures
- Risk Management
- Security Awareness Training
- Vendor & Third-Party Risk Management

Technical Controls

Technical solutions or mechanisms

- Identity & Access Management (IAM)
- Data Integrity
- Vulnerability Assessment & Management
- Patch Management
- Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)
- Endpoint Security
- Network Security/Segmentation
- Business Continuity Plan (BCP)
- Change Management
- Incidence Response & Management

Physical Controls

Measures to protect physical assets and infrastructures

- Security guards
- Biometric access systems
- Surveillance cameras
- Locks
- Picture IDs. Access cards

Cybersecurity Audit Process

Types of IT Audit

Financial Statement Audit

- Income Statement & Balance Sheet Audit

Internal Audit

- SOX Audit
- Operational Audit
- Compliance Audit
- Information Systems
- Audit Readiness

Cybersecurity Audit

- Cybersecurity Audit

Attestation Engagement

- SOC Audit

IT Audit Process

Phase 1:
Planning

Notification & request for
Preliminary information.
Kick Off Meeting

Phase 2:
Fieldwork

Walkthrough Meeting
Test of Design
Test of Operating Effectiveness
Status Meetings/Issue Validation

Phase 3:
Reporting

Draft Report
Management Response
Closing Meeting
Report Distribution

Phase 4:
Follow-Up

Follow-up & remediation

Planning Phase

Planning Phase

1. Determine the **Objective**, **Scope** and **Risk Considerations**

Planning Phase

1. Determine the **Objective - (The Why)**
    - Why are we conducting this test
        - Evaluate, determine, assess compliance
        - Determine certain goals are met
        - Assessing the reliability of data
        - Determine efficient use of resources
        - Evaluate safeguard of the organization’s assets

Planning Phase

1. Determine the **Audit Scope – (Where - When - What)**
    - Remote / On-premise
    - Time period / duration of audit
    - Specific areas of review
    - Sample size
    - Sampling methodology

Planning Phase

1. Determine any **Risk Considerations**

   - New systems or applications onboarded
   - New changes to industry regulations
   - Specific issues identified in previous testing

Planning Phase

1. Determine the objective audit scope and risk considerations
2. Applications to be tested are selected from the Application list
3. Team members are assigned work and responsibilities
4. Review past audit workpaper
5. Send notification & request for preliminary information & documents – PBC List (Prepared by Client)
6. Conduct Audit Kick-off meeting: (External Auditors & Internal Auditors)
    - Audit period
    - Questions about the PBC List / requested documents
    - Concerns needed to be addressed

Note: We can obtain/pull some or most of the requested items ourselves during fieldwork.

Fieldwork Phase

Fieldwork

1. Schedule meetings with application or process owners to discuss the audit request
2. Conduct a **Walkthrough** to understand the application or process

Walkthrough - Fieldwork

- Walkthrough is a process performed to gain understanding of the system, application or process being tested.
- Walkthrough involves following a transaction or process from initiation to its completion
  - Examine if the internal controls are properly designed
  - Observe if there is a control gap
  - Ask probing questions
  - Gather initial evidence
  - Perform a test of 1 – Test a single transaction from initiation to completion

Fieldwork Stage

1. Schedule meetings with application or process owner to discuss the audit request
2. Conduct a Walkthrough to understand the application or process – Test control design
3. Test the operating effectiveness of the controls by selecting a sample (e.g., 20% up to max 40)
4. Request evidence to support samples selected
5. Conduct status meetings with application/process owners – discuss findings/progress/delays/needs
6. Conduct weekly internal status meeting within internal audit (IA) team – status/progress/deliverables

Reporting Phase

Reporting Stage

1. No Control Deficiency identified
    - Document test steps and results
2. Control Deficiency identified
    - Prepare a draft report - list of audit findings or control weaknesses found
    - Request response from management
    - Management provides remediation plan
    - Final audit report is created
    - Distribute final audit report – Exit memo or Exit meeting

Follow-Up Phase

Follow-Up

1. Follow-up to determine if control deficiency have been corrected
2. Obtain evidence / re-test control
3. Close the deficiency

Performing Cybersecurity Audit

Internal Audit Team

Executives

Senior Director | Director

Controller/Manager **Controller/Manager**

Senior IT Auditors, IT Auditors, Associate IT Auditors | Senior Auditors, Auditors, Associate Auditors

Cybersecurity Audit

Sarbanes-Oxley (SOX) Audit

Operational Audit

Compliance Audit

Information Systems

Audit Readiness

Operational Audit

Compliance Audit

Business Operations Audit

Governance Audit

Audit Readiness

Internal Control Weakness

Control Test ⟷ Identify Weakness

Internal Control weakness are failures in the implementation or performance of internal controls

Internal Control Weakness

Control Design

Are the controls designed appropriately?

Control Effectiveness

Are the controls operating effectively?

Control Gap

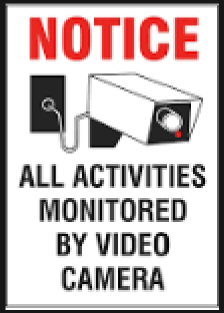
No control where we expect one to be

Identifying Control Weakness

Control Design
Are the controls designed appropriately?

The control has been thoughtfully developed to address specific risks or objectives

Store Break-In



NOTICE

ALL ACTIVITIES MONITORED BY VIDEO CAMERA

Risk: Future Break-In

Control: Surveillance Camera

Identifying Internal Control Weakness

Control Design
Are the controls designed appropriately?

Weak Password Policy

Risk: Unauthorized access

Control: Password

Identifying Control Weakness

Control Effectiveness
Are the controls operating effectively?

The control is consistently and successfully accomplishing its intended purpose

Store Break-In

Metal Door

Risk: Future Break-In

Control: Metal Door

Control Gap

No control where we expect one to be

A control does not exist where we expect a control to be present

Self Checkout

Risk: Shoppers not paying for items

Control: Employee stationed at Self-Checkout

Identifying Control Weakness

Control Design

Are the controls designed appropriately?

Control Effectiveness

Are the controls operating effectively?

Control Gap

No control where we expect one to be

Performing Cybersecurity Audit

IT Audit Process

Phase 1: Planning

Notification & request for
Preliminary information.
Kick Off Meeting

Phase 2: Fieldwork

Walkthrough Meeting
Test of Design
Test of Operating Effectiveness
Status Meetings/Issue Validation

Step 3: Reporting

Draft Report
Management Response
Closing Meeting
Report Distribution

Step 4: Follow-Up

Follow-up & remediation

Planning

Planning Phase

1. Determine the **Audit Scope – (Where - When - What)**

    - Remote / On-premise
    - Time period / duration of audit
    - Specific areas of review
    - Sample size
    - Sampling methodology

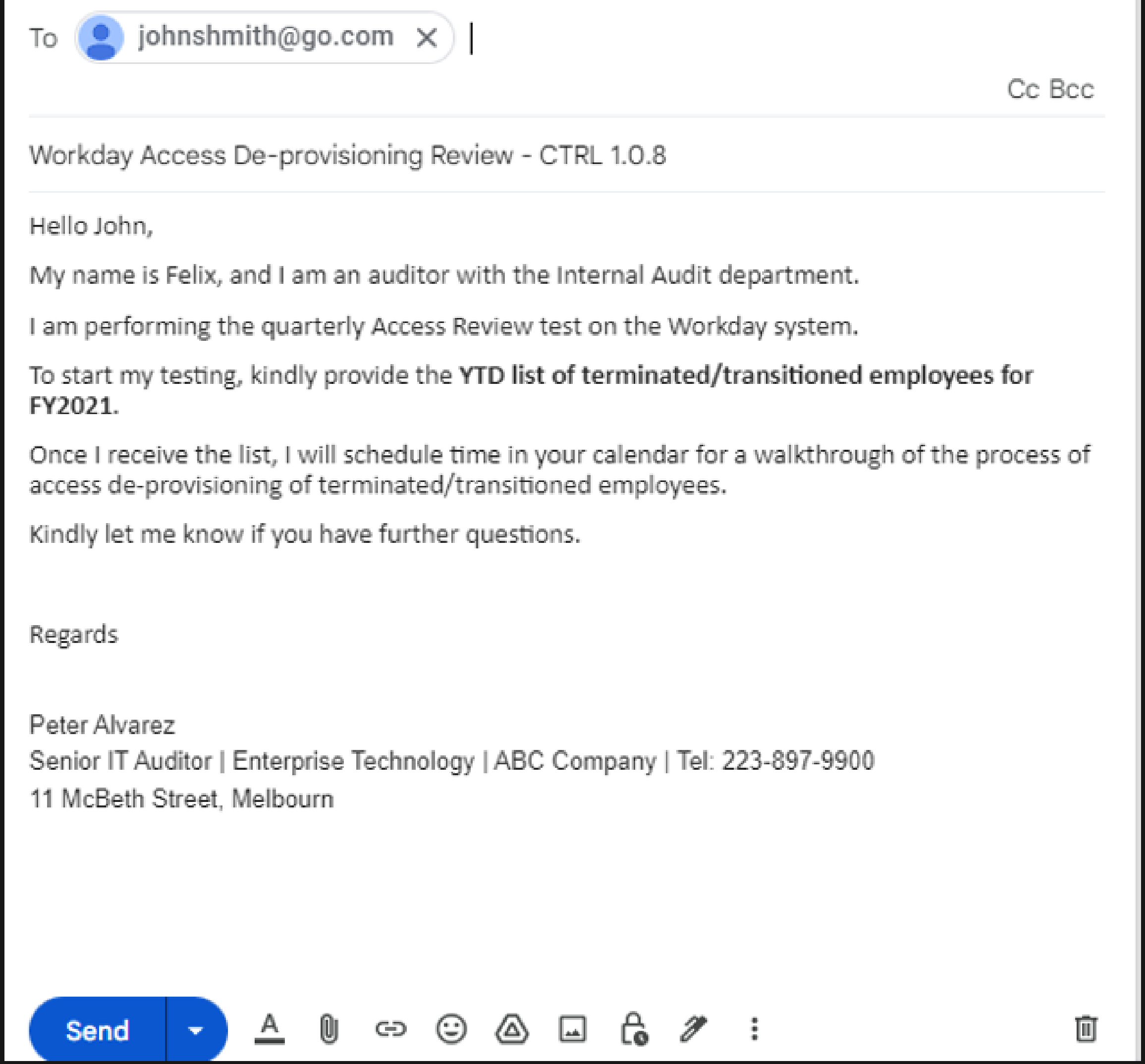
Planning Phase

1. Determine the objective audit scope and risk considerations
2. Applications and controls to be tested are selected from the Application list and control matrix
3. Team members are assigned work and responsibilities
4. Review past audit workpaper
5. Send notification & request for preliminary information & documents – PBC List (Prepared by Client)
6. Conduct Audit Kick-off meeting:
   - Audit period
   - Questions about the PBC List / requested documents
   - Concerns needed to be addressed

Fieldwork

Fieldwork

1. Schedule meetings with application or process owners to discuss the audit request



Workday Access De-provisioning Review - CTRL 1.0.8

Hello John,

My name is Felix, and I am an auditor with the Internal Audit department.

I am performing the quarterly Access Review test on the Workday system.

To start my testing, kindly provide the **YTD list of terminated/transitioned employees for FY2021**.

Once I receive the list, I will schedule time in your calendar for a walkthrough of the process of access de-provisioning of terminated/transitioned employees.

Kindly let me know if you have further questions.

Regards

Peter Alvarez
Senior IT Auditor | Enterprise Technology | ABC Company | Tel: 223-897-9900
11 McBeth Street, Melbourn

Fieldwork

1. Schedule meetings with application or process owners to discuss the audit request
2. Conduct a **Walkthrough** to understand the application or process
    - Follow a transaction or process from initiation to completion
    - Inspect processes or documentations
    - Ask probing questions
    - Observe if there is a control gap
  - Gather initial evidence
  - Perform a Test of 1 – Test a single transaction from initiation to completion

Fieldwork Stage

1. Schedule meetings with application or process owner to discuss the audit request
2. Conduct a Walkthrough to understand the application or process – Test control design
3. Test the operating effectiveness of the controls by selecting a sample (e.g., 20% up to max 40)
4. Request evidence to support samples selected
5. Review evidence provided
6. Conduct status meetings with application/process owners – discuss findings/progress/delays/needs
7. Conduct weekly internal status meeting within internal audit (IA) team – status/progress/deliverables

Testing Technical Controls During Fieldwork

Technical Controls

Technical solutions or mechanisms

- Identity & Access Management (IAM)
- Data Integrity
- Vulnerability Assessment & Management
- Patch Management
- Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)
- Endpoint Security
- Network Security/Segmentation
- Business Continuity Plan (BCP)
- Change Management
- Incidence Response & Management

Identity & Access Management (IAM) Testing

Identity & Access Management Controls

- Password configuration
- User Access authorization
  - Access provisioning
  - Access deprovisioning
- General User access
- Privileged Access Management
- User Access Reviews
- Segregation of Duties (SOD)

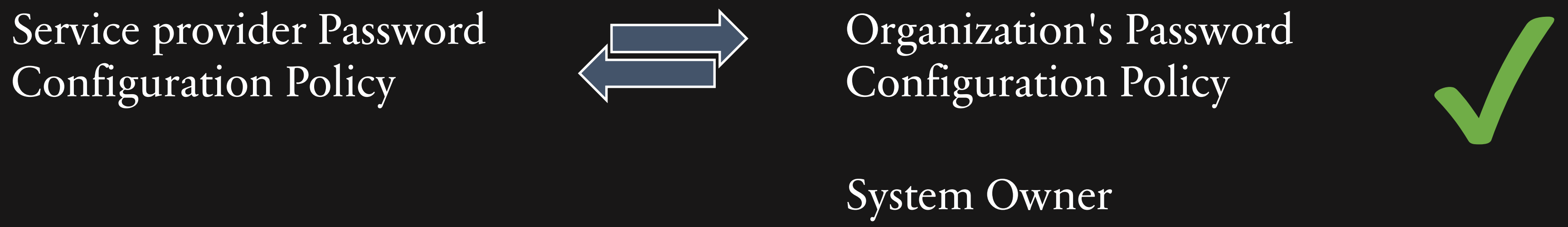
Password Configuration

Password Configuration Testing - IAM Controls

Control Testing

- Confirm one-time password for initial log on to application
- Verify password has a minimum character length
- Verify password composition contains alpha/numeric characters
- Password expires after 90 days
- Confirm password history prior to reusing a password
- Determine limit on the number of unsuccessful attempts to sign on

Password Configuration Test Result



Service provider Password Configuration Policy

Organization's Password Configuration Policy

System Owner

Service Provider Policy:
Password length minimum of 6 characters

Organization’s Policy:
Password length must have a minimum of 8 characters

User Access Authorization

Access Provisioning – IAM Controls

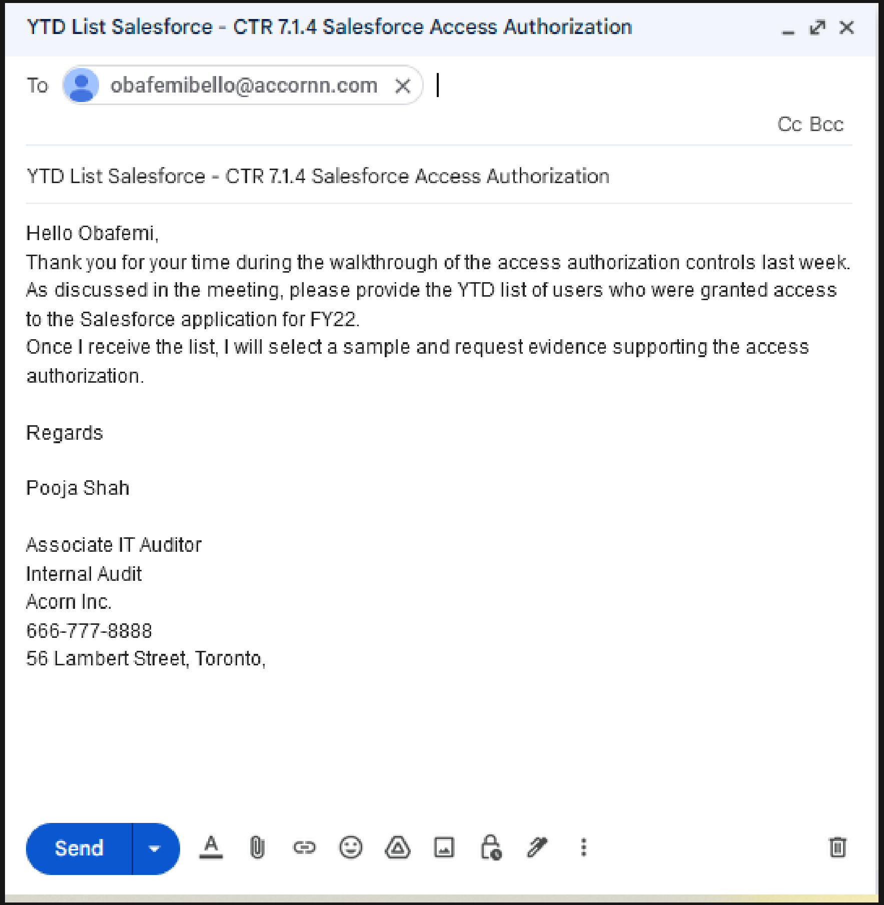
Control Testing

- Determine the access approval process
- Obtain evidence of access request and approval from appropriate persons
- Verify that employees are only granted access to systems/application in line with job function

Access Provisioning – IAM Controls

Control Testing

- Request list of access granted within audit period



YTD List Salesforce - CTR 7.1.4 Salesforce Access Authorization

To obafemibello@accornn.com

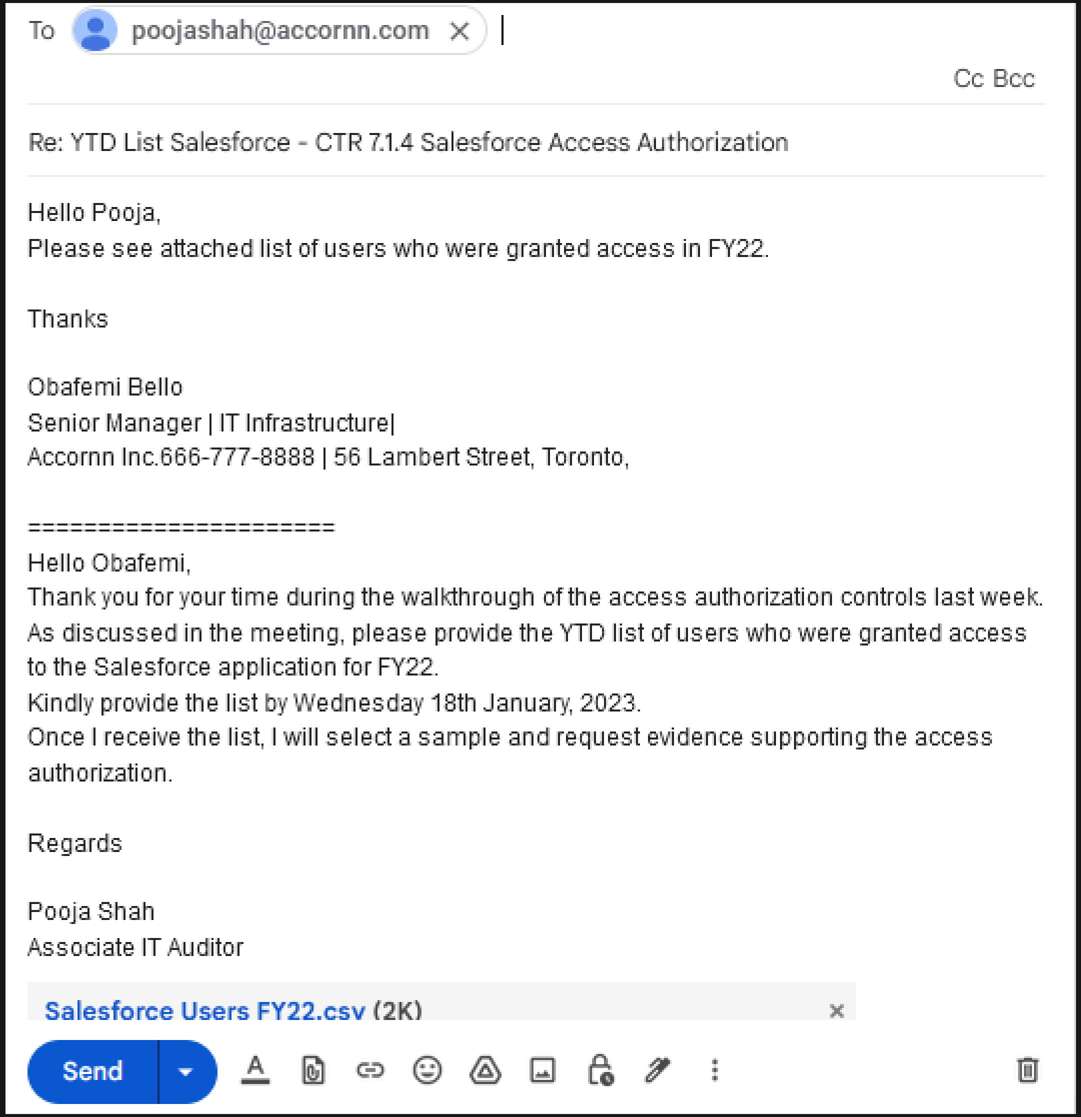
YTD List Salesforce - CTR 7.1.4 Salesforce Access Authorization

Hello Obafemi,
Thank you for your time during the walkthrough of the access authorization controls last week.
As discussed in the meeting, please provide the YTD list of users who were granted access to the Salesforce application for FY22.
Once I receive the list, I will select a sample and request evidence supporting the access authorization.

Regards

Pooja Shah

Associate IT Auditor
Internal Audit
Acorn Inc.
666-777-8888
56 Lambert Street, Toronto,



To poojashah@accornn.com

Re: YTD List Salesforce - CTR 7.1.4 Salesforce Access Authorization

Hello Pooja,
Please see attached list of users who were granted access in FY22.

Thanks

Obafemi Bello
Senior Manager | IT Infrastructure|
Accornn Inc.666-777-8888 | 56 Lambert Street, Toronto,

======================
Hello Obafemi,
Thank you for your time during the walkthrough of the access authorization controls last week.
As discussed in the meeting, please provide the YTD list of users who were granted access to the Salesforce application for FY22.
Kindly provide the list by Wednesday 18th January, 2023.
Once I receive the list, I will select a sample and request evidence supporting the access authorization.

Regards

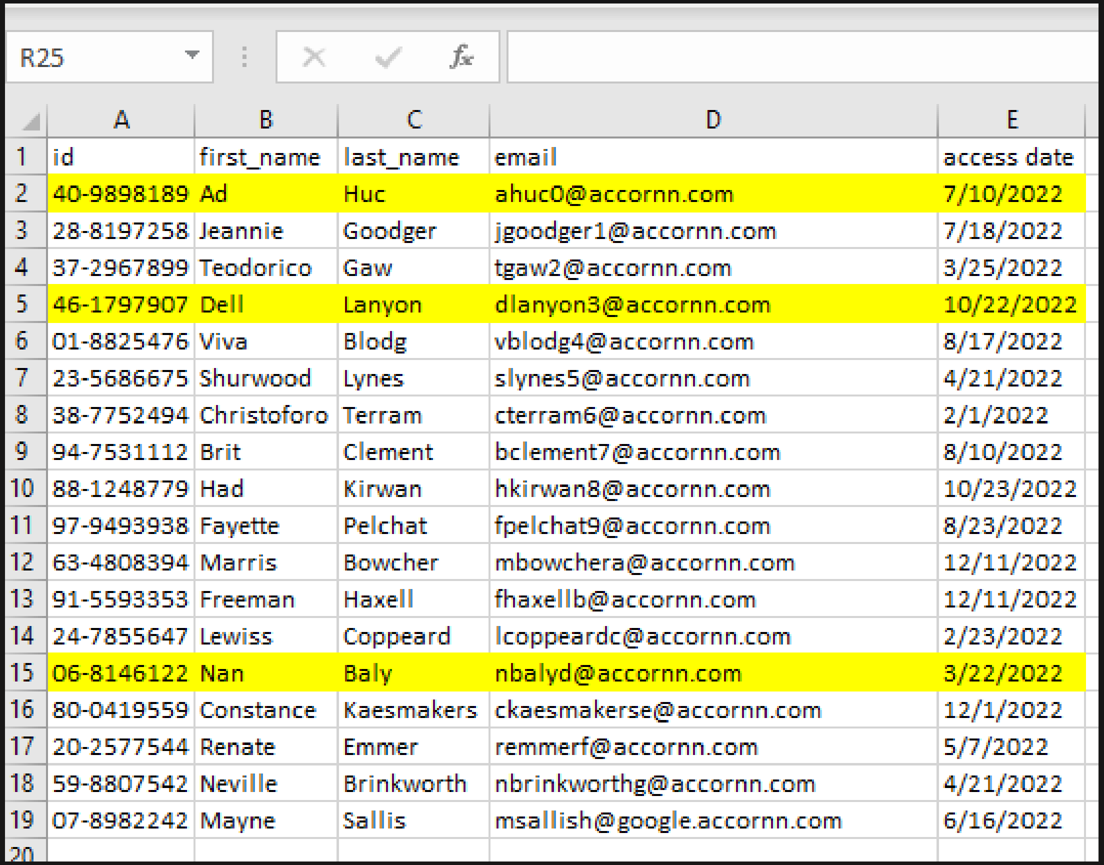
Pooja Shah
Associate IT Auditor

Salesforce Users FY22.csv (2K)

Access Provisioning – IAM Controls

Control Testing

- Select sample from population to test (10% to max of 25 transactions)



	A	B	C	D	E
1	id	first_name	last_name	email	access date
2	40-9898189	Ad	Huc	ahuc0@accornn.com	7/10/2022
3	28-8197258	Jeannie	Goodger	jgoodger1@accornn.com	7/18/2022
4	37-2967899	Teodorico	Gaw	tgaw2@accornn.com	3/25/2022
5	46-1797907	Dell	Lanyon	dlanyon3@accornn.com	10/22/2022
6	01-8825476	Viva	Blodg	vblodg4@accornn.com	8/17/2022
7	23-5686675	Shurwood	Lynes	slynes5@accornn.com	4/21/2022
8	38-7752494	Christoforo	Terram	cterram6@accornn.com	2/1/2022
9	94-7531112	Brit	Clement	bclement7@accornn.com	8/10/2022
10	88-1248779	Had	Kirwan	hkirwan8@accornn.com	10/23/2022
11	97-9493938	Fayette	Pelchat	fpelchat9@accornn.com	8/23/2022
12	63-4808394	Marris	Bowcher	mbowchera@accornn.com	12/11/2022
13	91-5593353	Freeman	Haxell	fhaxellb@accornn.com	12/11/2022
14	24-7855647	Lewiss	Coppeard	lcoppeardc@accornn.com	2/23/2022
15	06-8146122	Nan	Baly	nbalyd@accornn.com	3/22/2022
16	80-0419559	Constance	Kaesmakers	ckaesmakerse@accornn.com	12/1/2022
17	20-2577544	Renate	Emmer	remmerf@accornn.com	5/7/2022
18	59-8807542	Neville	Brinkworth	nbrinkworthg@accornn.com	4/21/2022
19	07-8982242	Mayne	Sallis	msallish@google.accornn.com	6/16/2022
20					

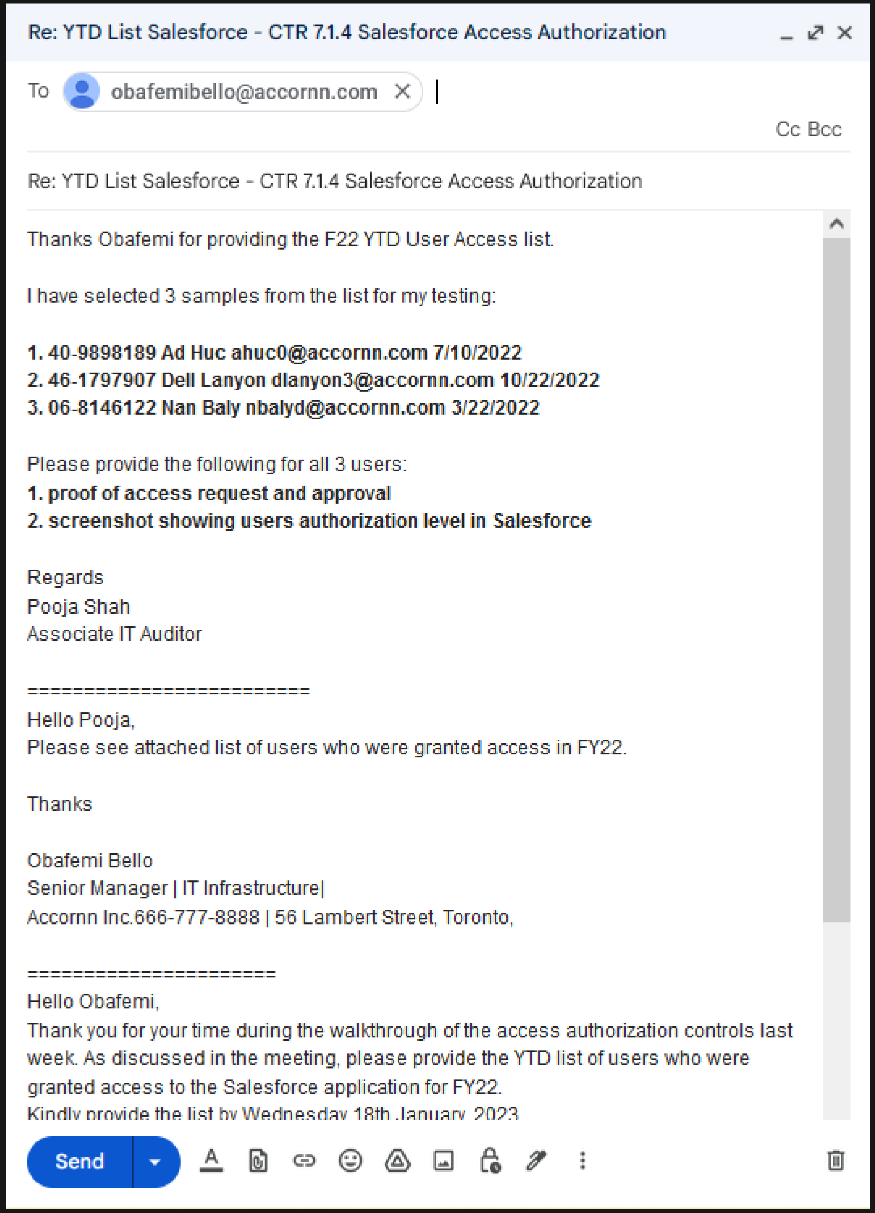
Access Provisioning – IAM Controls

Control Testing

- Obtain evidence of access request/approval from appropriate persons

- Verify that employees were only granted access to systems/application in line with job function

- Verify that access granted by the system administrator is in line with approval



Re: YTD List Salesforce - CTR 7.1.4 Salesforce Access Authorization

To: obafemibello@accornn.com

Re: YTD List Salesforce - CTR 7.1.4 Salesforce Access Authorization

Thanks Obafemi for providing the F22 YTD User Access list.

I have selected 3 samples from the list for my testing:

1. 40-9898189 Ad Huc ahuc0@accornn.com 7/10/2022
2. 46-1797907 Dell Lanyon dlanyon3@accornn.com 10/22/2022
3. 06-8146122 Nan Baly nbalyd@accornn.com 3/22/2022

Please provide the following for all 3 users:
1. proof of access request and approval
2. screenshot showing users authorization level in Salesforce

Regards
Pooja Shah
Associate IT Auditor

==========================
Hello Pooja,
Please see attached list of users who were granted access in FY22.

Thanks

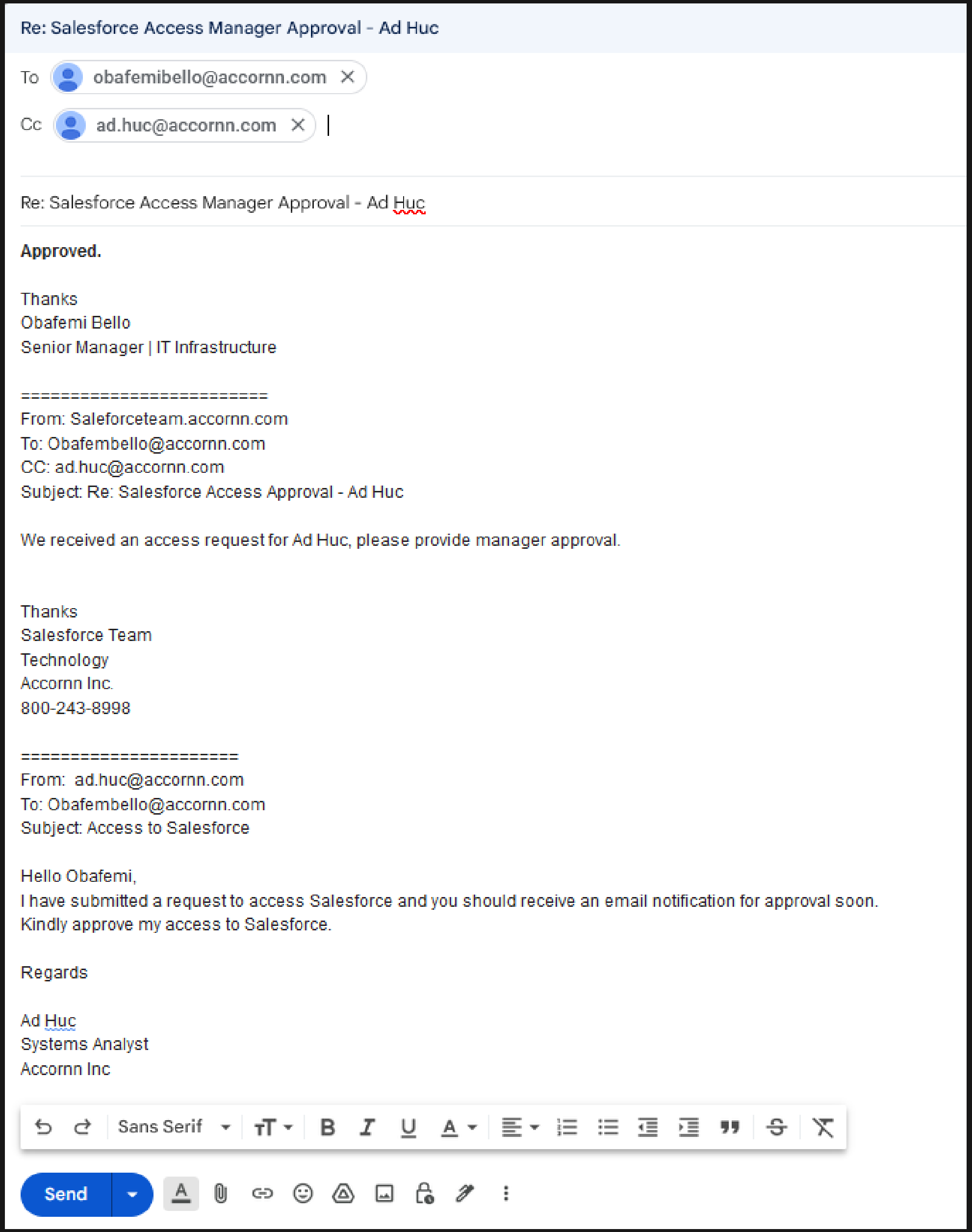
Obafemi Bello
Senior Manager | IT Infrastructure|
Accornn Inc.666-777-8888 | 56 Lambert Street, Toronto,

=======================
Hello Obafemi,
Thank you for your time during the walkthrough of the access authorization controls last week. As discussed in the meeting, please provide the YTD list of users who were granted access to the Salesforce application for FY22.
Kindly provide the list by Wednesday 18th January 2023

Access Provisioning – IAM Controls

Control Testing

- Obtain evidence of access request/approval from appropriate persons
- Verify that employees were only granted access to systems/application in line with job function
- Verify that access granted by the system administrator is in line with approval



Re: Salesforce Access Manager Approval - Ad Huc

To obafemibello@accornn.com

Cc ad.huc@accornn.com

Re: Salesforce Access Manager Approval - Ad Huc

Approved.

Thanks
Obafemi Bello
Senior Manager | IT Infrastructure

========================
From: Saleforceteam.accornn.com
To: Obafembello@accornn.com
CC: ad.huc@accornn.com
Subject: Re: Salesforce Access Approval - Ad Huc

We received an access request for Ad Huc, please provide manager approval.

Thanks
Salesforce Team
Technology
Accornn Inc.
800-243-8998

=====================
From: ad.huc@accornn.com
To: Obafembello@accornn.com
Subject: Access to Salesforce

Hello Obafemi,
I have submitted a request to access Salesforce and you should receive an email notification for approval soon.
Kindly approve my access to Salesforce.

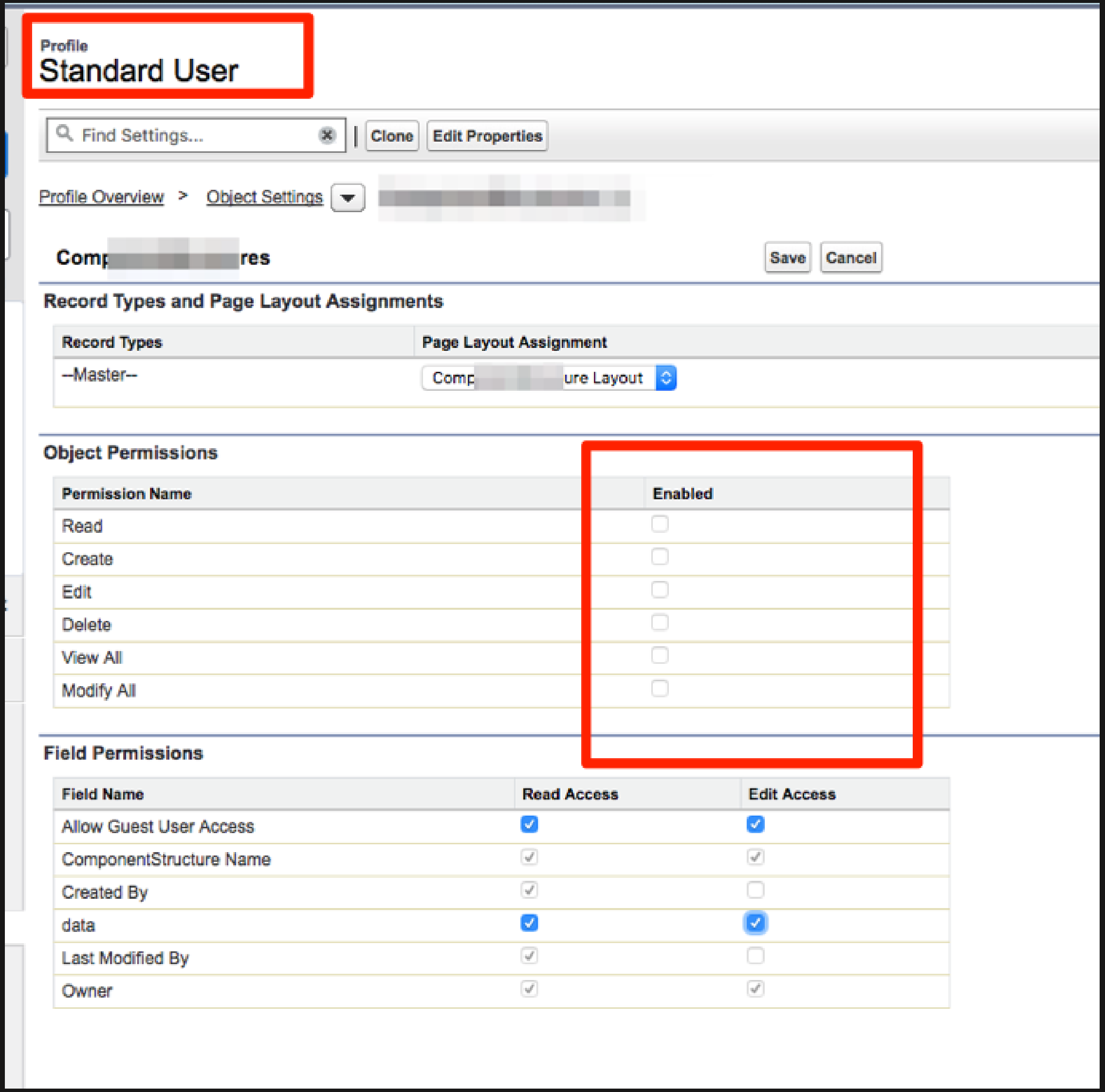
Regards

Ad Huc
Systems Analyst
Accornn Inc

Access Provisioning – IAM Controls

Control Testing

- Obtain evidence of access request/approval from appropriate persons
- Verify that employees were only granted access to systems/application in line with job function
- Verify that access granted by the system administrator is in line with approval



Profile

Standard User

Profile Overview > Object Settings [redacted]

Comp[redacted]res

Record Types and Page Layout Assignments

Record Types	Page Layout Assignment
--Master--	Comp[redacted]ure Layout

Object Permissions

Permission Name	Enabled
Read	□
Create	□
Edit	□
Delete	□
View All	□
Modify All	□

Field Permissions

Field Name	Read Access	Edit Access
Allow Guest User Access	☑	☑
ComponentStructure Name	☑	☑
Created By	☑	□
data	☑	☑
Last Modified By	☑	□
Owner	☑	☑

Access De-provisioning – IAM Controls

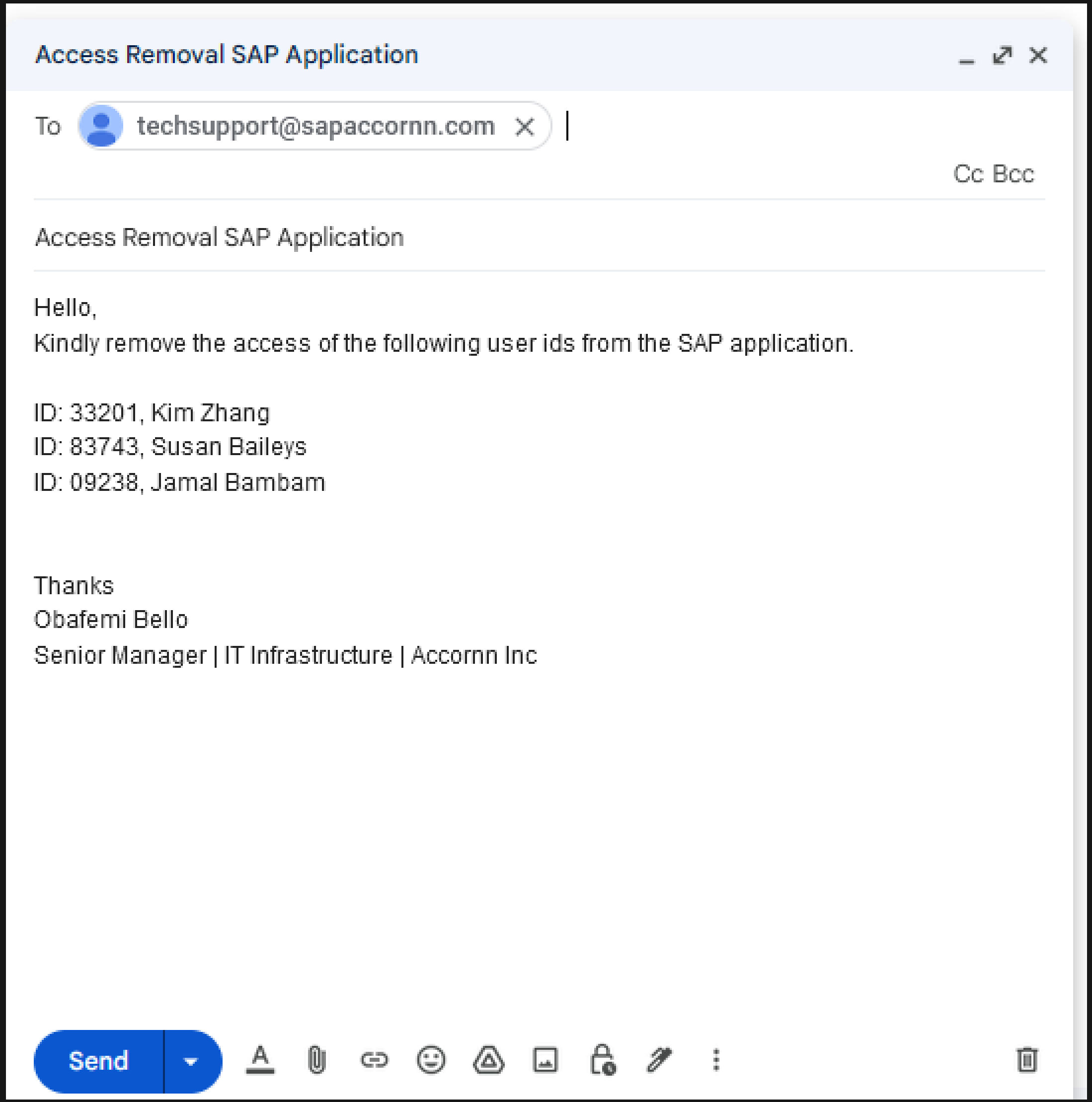
Control Testing

- Determine the process for revoking access
- Obtain list of terminated employees
- Obtain evidence of access removal request
- Obtain evidence that access was removed from all systems and applications
- Obtain evidence access was remove timely (Based on organization’s policy)

Access De-provisioning – IAM Controls

Control Testing

- Obtain evidence of user's access review
- Obtain evidence of access removal request



Access Removal SAP Application

Hello,
Kindly remove the access of the following user ids from the SAP application.

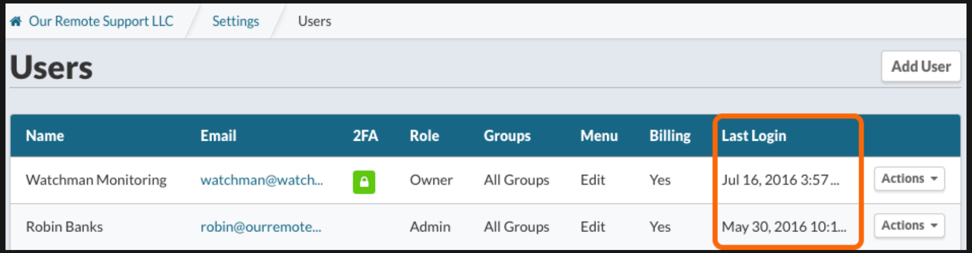
ID: 33201, Kim Zhang
ID: 83743, Susan Baileys
ID: 09238, Jamal Bambam

Thanks
Obafemi Bello
Senior Manager | IT Infrastructure | Accornn Inc

Access De-provisioning – IAM Controls

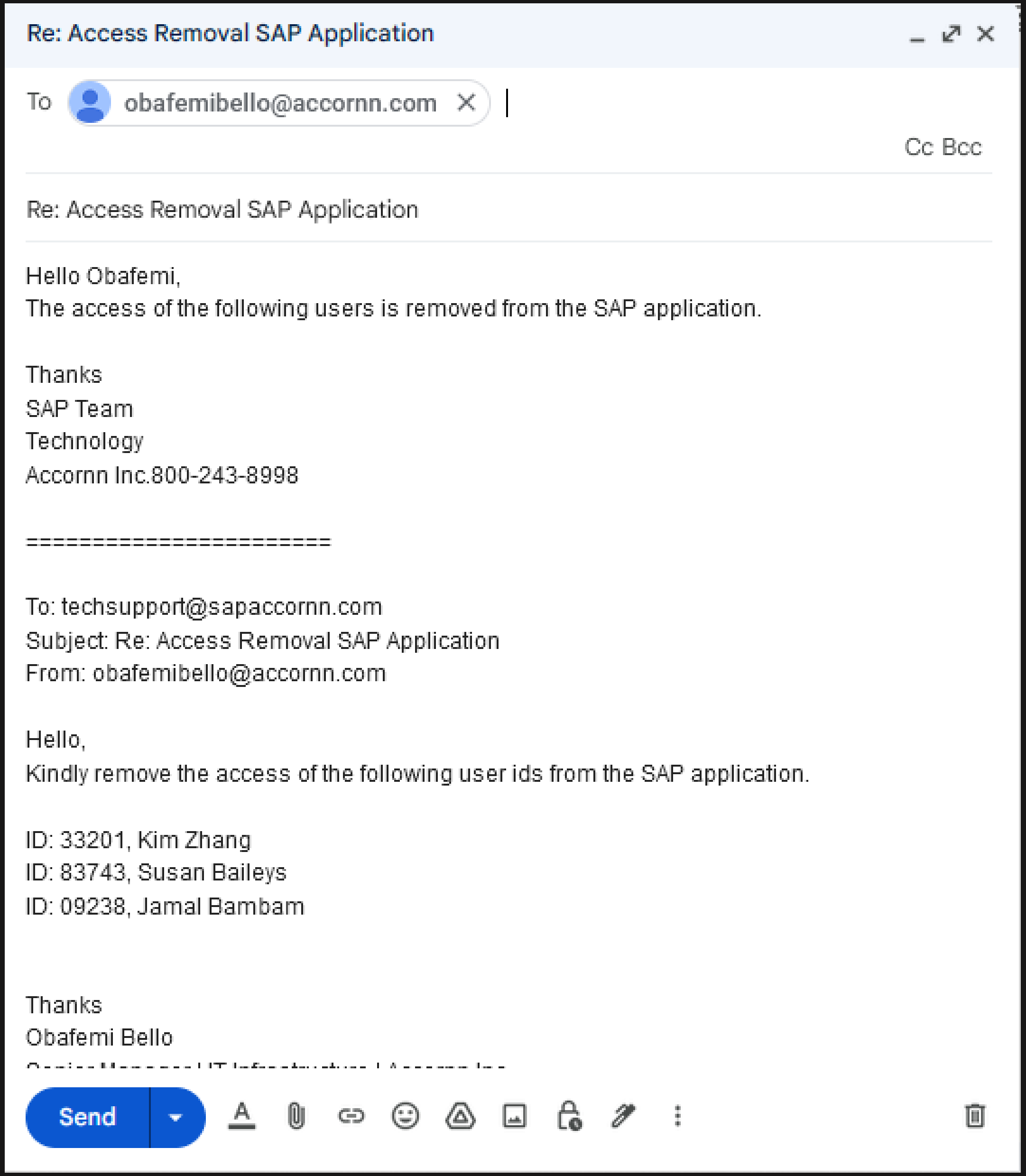
Control Testing

- Obtain evidence that the all access was removed from applications and systems



Users

Name	Email	2FA	Role	Groups	Menu	Billing	Last Login	
Watchman Monitoring	watchman@watch...	🔒	Owner	All Groups	Edit	Yes	Jul 16, 2016 3:57...	Actions ▾
Robin Banks	robin@ourremote...		Admin	All Groups	Edit	Yes	May 30, 2016 10:1...	Actions ▾



Re: Access Removal SAP Application

To obafemibello@accornn.com

Re: Access Removal SAP Application

Hello Obafemi,
The access of the following users is removed from the SAP application.

Thanks
SAP Team
Technology
Accornn Inc.800-243-8998

=======================

To: techsupport@sapaccornn.com
Subject: Re: Access Removal SAP Application
From: obafemibello@accornn.com

Hello,
Kindly remove the access of the following user ids from the SAP application.

ID: 33201, Kim Zhang
ID: 83743, Susan Baileys
ID: 09238, Jamal Bambam

Thanks
Obafemi Bello
Senior Manager | IT Infrastructure | Accornn Inc

Privileged Access Testing

Privileged Access Management Controls Testing

Privileged Users

System administrator, database administrator, network administrator, developers

Elevated Permissions

Ability to create, modify, delete or access critical data

Security Risks

Privileged accounts poses higher security risks

Privileged Access Controls Testing

Control Testing

- Determine privileged user approval process
- Obtain evidence of privileged access request
- Obtain evidence of privileged access approval from appropriate persons
- Obtain evidence of privileged access review (Usually performed quarterly)

Segregation of Duties (SOD)

Segregation of Duties (SOD)

- Segregation of Duties help minimize error or fraud
- Individuals performing certain control activities should not have conflicting duties.
- Segregation of Duties involves separating three main functions:
  - Having custody of assets
  - Being able to authorize the use of assets
  - Recordkeeping of assets

Segregation of Duties (SOD) Control Testing

Control Testing

- Determine that individuals performing the control activities over user access do not have conflicting duties
- Determine that different individual perform the following duties related to logical access:
  - Requesting access
  - Approving access
  - Setting up access
- Obtain evidence of compensating controls where Segregation of Duties cannot be achieved

Data Integrity

Data integrity are security measures and mechanism organizations put in place to ensure the accuracy, consistency, and reliability of their data.

Data Integrity Controls Testing

Why maintain Data Integrity?

Organization usually make data driven decisions

Data Integrity Threats

Human error

Unintended transfer errors

Misconfigurations and security errors

Malware, insider threats, and cyberattacks

Compromised hardware

Data Integrity Controls Testing

Control Testing

- Data retention and disposal procedure are in place.
- Data encryption/cryptography is utilized
- Data validation checks – input, processing and output controls
- Physical & logical access controls to databases, data centre and server rooms
- Anti-virus software is installed on servers and workstations
- Data is backed-up and can be recovered when needed

Vulnerability Assessment & Management

Vulnerability management involves assessing and mitigating vulnerabilities in an organizations information systems and networks

Vulnerability Assessment & Management

Vulnerability Assessment

Discover vulnerabilities

Assign severity level

Recommend mitigation or remediation

Types of Vulnerability Assessments

Network Scan: Identifies vulnerable systems on organizations' wired and wireless networks

Host-based Scan: Identifies potential vulnerabilities in critical servers and workstations

Wireless Scan: Assesses organization's WI-FI connections and network configuration

Application Scan: Tests an organization's websites for known software vulnerabilities and weak configurations in web applications or networks

Database Scan: Identifies weaknesses in databases and systems configuration

Vulnerability Assessment & Management Controls Testing

Control Testing

- Check whether automated vulnerability scanning tools are in place
- Verify regular vulnerability scans are performed on the network, servers and applications
- Check if identified vulnerabilities are properly categorized and assessed for risk
- Verify that there is defined timelines for addressing critical vulnerabilities

Patch Management

Patch management focuses on evaluating an organization's processes and controls for managing software patches and updates

Patch Management Controls Testing

Control Testing

- Check whether there are documented procedures for testing patches before deployment
- Test if patches are applied in a timely manner based on their criticality
- Confirm comprehensive documentation of patches
- Confirm if patches are evaluated and tested for potential impact before installation
- Verify if issues and incidents are documented and resolved appropriately

Firewall & Intrusion Detection & Prevention Systems

Focuses on evaluating an organization's firewall infrastructure and its effectiveness in protecting the network from unauthorized access, threats, and cyberattacks

Firewall Management Controls Testing

Control Testing

- Confirm that the firewall configuration settings align with security best practices and the organization's security policies.
- Verify that firewall rules are documented and regularly reviewed
- Confirm that firewall administrators regularly perform rule cleanup
- Confirm if alerts are generated and reviewed for suspicious or anomalous activities.

End-Point Security

Ensure that endpoints are adequately protected against threats and vulnerabilities.

Endpoint Security (Computers, Laptops, Smart Phones) Controls Testing

Control Testing

- Verify the use of endpoint detection and response (EDR) solutions
- Verify the presence of up-to-date antivirus and anti-malware software on endpoints.
- Confirm that operating systems and software on endpoints are patched and updated regularly.
- Verify that critical security patches are deployed promptly.
- Verify that endpoint firewall settings are properly configured.

Network Security

Prevent unauthorized network access and intrusion while safeguarding digital assets present within the network

Network Controls Testing

Control Testing

- Verify if all network devices are managed according to a documented policy or procedure
- Network access controls
- Verify if confidential data are encrypted across networks
- Verify if wireless network communications are encrypted
- Confirm if a network diagram showing network segmentation is accurately maintained
- Penetration Testing, System Hardening & Firewall Testing
- Vulnerability assessment and scanning

Business Continuity Plan (BCP)

BCP Plan details critical steps and activities an organization must follow in the event of an emergency

Business Continuity Plan (BCP) Controls Testing

Control Testing

- Obtain evidence the organization conduct a yearly review & testing of their BCP
- Verify if Disaster Recovery Plan has been tested for the audit period
- Verify if regular back-up of data is implemented
- Verify if back-up recovery has been tested for the audit period
- Verify if a Business Impact Analysis was conducted in the past 12 months
- Verify if identified issues were resolved and the BCP plan updated accordingly

Change Management

Ensures changes made to an organization's IT infrastructure, systems, applications, or processes do not adversely affect the stability, security, or functionality of the environment.

Business Continuity Plan (BCP) Controls Testing

Control Testing

- Confirm if the organization have a change management policy
- Request for Change Orders (CO) and verify:
    - Formal request for change
    - Formal approval of change
    - Appropriate testing before deployment to production – UAT, QA test, Code reviews
- Incident management process
- Test segregation of duties:
    - Requestor
    - Approver of change
    - Change developers
    - Promoting change to production

Incident Management & Tracking

Identifying, logging, tracking, and resolving incidents in an organization's IT environment.

Incident Management & Tracking

Incidents

Unplanned events that disrupt normal IT service operations and negatively impact business processes

Key Aspects of Incident Management Tracking

Incident Identification

Logging & Documentation

Categorization & prioritization

Assignment & Notification

Resolution & Verification

Closure

Incident Management & Tracking Controls Testing

Control Testing

- Confirm if an Incident Management policy exist
- Verify that the organization have an Incident Management System:
  - Incident identification
  - Incident logging and documentation
  - Categorization and Prioritization
  - Resolution and Verification
- Communication

Operational Controls

Operational Controls

Policies & procedures established to manage & govern security practices

- Policies and Procedures
- Risk Assessment & Management
- Security Awareness Training
- Vendor & Third-Party Risk Management

Policies & Procedures

Rules, guidelines and procedures to protect IT systems, data, network and digital assets from cyber threats and security breaches

Cybersecurity Policies

Control Testing

- Password policy
- Data classification & handling policy
- Access control policy
- Incident response policy
- Network security policy
- Security awareness & training policy
- Data backup & recovery policy
- Security incident reporting policy
- Encryption policy
- Software & patch management policy
- Compliance & regulatory policy

Risk Assessment & Management

Identify, assess, and prioritize risks to information and information systems.

Cybersecurity Risk Assessment

- Determine the scope of the risk assessment
- Identify cybersecurity risks
  - Identify assets
  - Identify threats
  - Identify what could go wrong
- Analyze risks and determine potential impact
- Evaluate the risks
- Prioritize the risks
- Risk treatment
- Document findings

Risk Assessment Control Testing

Control Testing

- Request evidence of risk assessment performed on in-scope applications and systems
- Confirm if identified risks are managed along with appropriate controls
- Confirm if a process of communicating security incident to customers exist
- Verify if identified risks are tracked to closure
- Verify if identified risk issues are remediated on time

Security Awareness Training

Employees, contractors, and other stakeholders are knowledgeable about cybersecurity best practices and can recognize and respond to potential security threats.

Security Awareness Training

Key Training Components

Phishing Simulations

Social Engineering Exercises

Password Security

Device & Physical Security

Data Protection

Incident Reporting

Secure Communication

Data Privacy & Compliance

Regulatory Compliance

Security Awareness Training Control Testing

Control Testing

- Request confirmation that selected employee completed the annual Security Awareness Training

Vendor & Third-Party Risk Management

Ensure that third party vendors meet the security standards and contractual requirements to protect the organization's sensitive information and digital assets.

Vendor & Third-Party Risk Management Controls Testing

Control Testing

- Vendor & Third-Party Security Policy
- Confirm that all vendor patches are being applied to environments according to required timelines
- Obtain Service Organization Controls (SOC) Report of vendors & service providers

Physical Access Controls

Protect the physical infrastructure, data centers, offices, and other areas from unauthorized access

Physical Access Controls Testing is generally

Out of Scope for Cybersecurity Audit

Physical Controls

Measures to protect physical assets and infrastructures

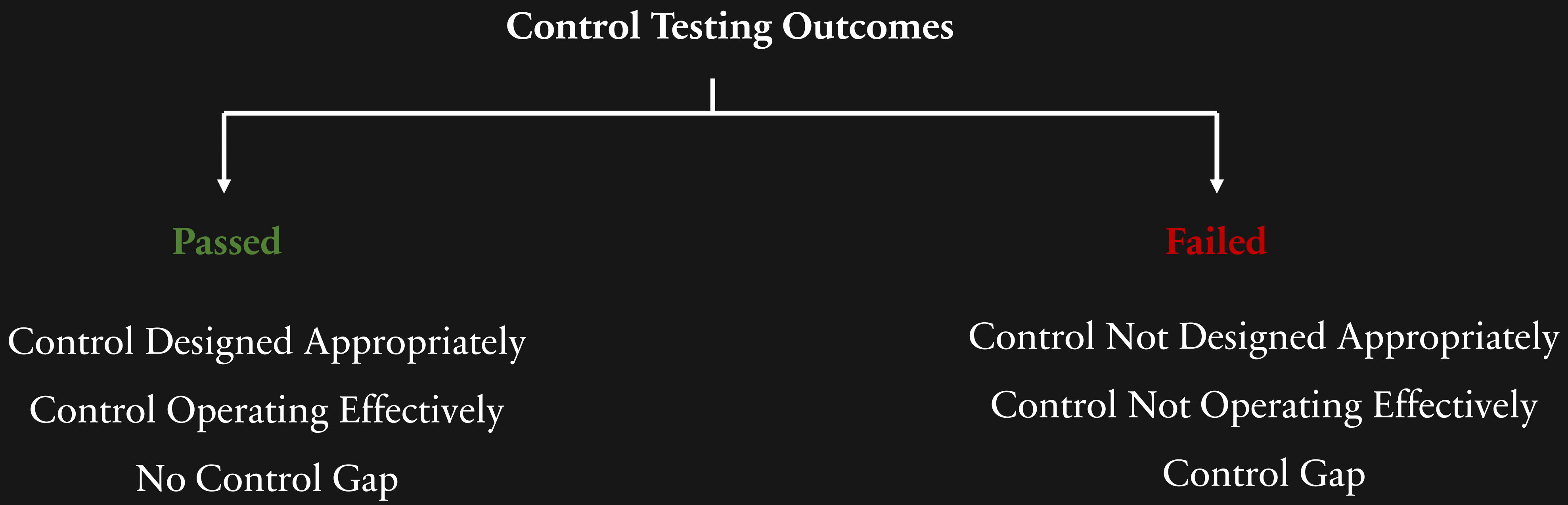
- Security Guards
- Biometric Access Systems
- Surveillance Cameras
- Locks
- Picture IDs. Access cards
- Visitors' Management
- Emergency Access Testing

Reporting Phase

Documenting and communicating the findings, results, and recommendations derived from the audit to relevant stakeholders, including management, executives, and relevant teams.

Cybersecurity Audit Testing Outcomes

Cybersecurity Audit Testing Outcomes



Control Testing Outcomes

Passed

Control Designed Appropriately

Control Operating Effectively

No Control Gap

Failed

Control Not Designed Appropriately

Control Not Operating Effectively

Control Gap

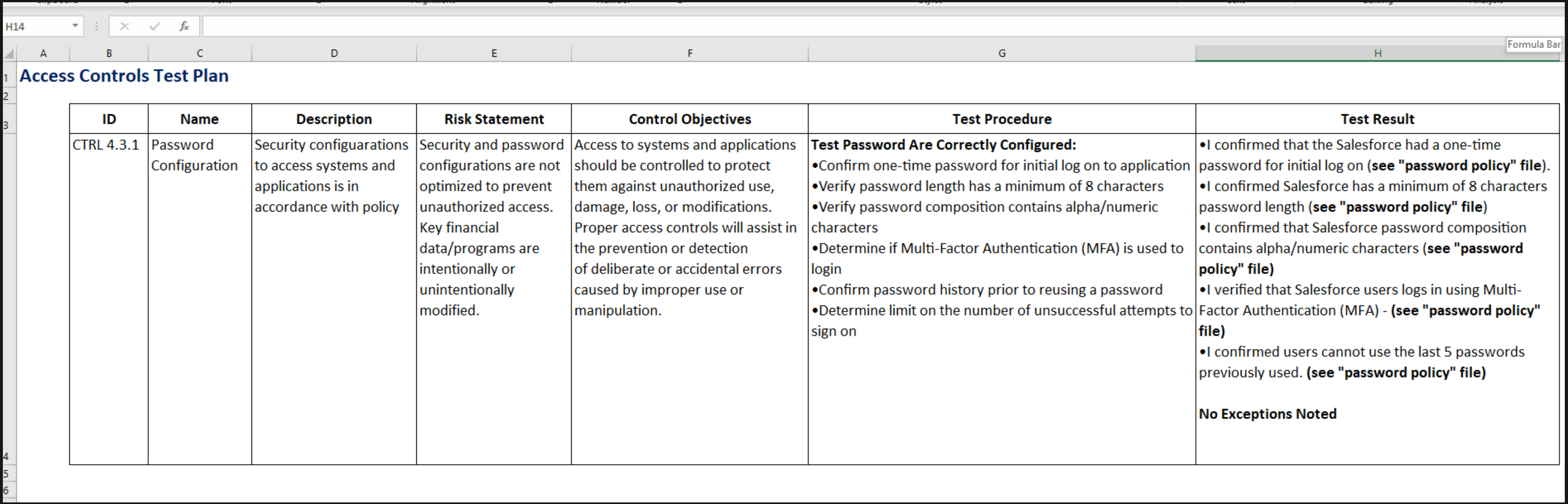
Control Deficiency

Control Deficiency exist when the design or operation of a control does not prevent or detect the likelihood of security breaches, errors, operational failures or financial misstatement

Reporting Test Results

Reporting Format – Internal Audit Department

- Document test steps & results using Excel, Google Sheets, Word, PowerPoint
- IT Audit software applications – Auditboard, monitorQA, iAuditor, Highbond etc..



Access Controls Test Plan

ID	Name	Description	Risk Statement	Control Objectives	Test Procedure	Test Result
CTRL 4.3.1	Password Configuration	Security configuarations to access systems and applications is in accordance with policy	Security and password configurations are not optimized to prevent unauthorized access. Key financial data/programs are intentionally or unintentionally modified.	Access to systems and applications should be controlled to protect them against unauthorized use, damage, loss, or modifications. Proper access controls will assist in the prevention or detection of deliberate or accidental errors caused by improper use or manipulation.	**Test Password Are Correctly Configured:** •Confirm one-time password for initial log on to application •Verify password length has a minimum of 8 characters •Verify password composition contains alpha/numeric characters •Determine if Multi-Factor Authentication (MFA) is used to login •Confirm password history prior to reusing a password •Determine limit on the number of unsuccessful attempts to sign on	•I confirmed that the Salesforce had a one-time password for initial log on (**see "password policy" file**). •I confirmed Salesforce has a minimum of 8 characters password length (**see "password policy" file**) •I confirmed that Salesforce password composition contains alpha/numeric characters (**see "password policy" file)** •I verified that Salesforce users logs in using Multi-Factor Authentication (MFA) - **(see "password policy" file)** •I confirmed users cannot use the last 5 passwords previously used. **(see "password policy" file)** **No Exceptions Noted**

Reporting on Control Deficiency

Examples of Deficiencies

- **Access Controls**
  - Poor user access review
  - Password not properly configured
  - Inadequate role-based access control
  - User access not revoked at all or not revoked timely
  - No segregation of duties between approver and implementer
- **Change Management Controls**
  - Lack of documented change management policies and procedures
  - Inadequate change approval process
  - Lack of testing and validation
  - Inadequate monitoring and reporting
  - No segregation of duties between approver and implementer

Risk Assessment

- Risk Assessment is conducted to determine potential impact
  - Low Risk
  - Medium Risk
  - High Risk

Control Deficiency & Risk Levels

Risk Level	Action
Low	Client can take time to remediate the deficiency
Medium	Need to be corrected as soon as possible & management needs to know about it
High	Need to be corrected immediately & management needs to know about it

Reporting Deficiencies

- Prepare a draft report - list of audit findings or control weaknesses found
- Audit team reviews the audit report
- Draft report sent to management
- Request response from management
  - Remediation plan
  - Timeline to remediate deficiency
- Final changes made to audit report
- Distribute final audit report

Follow-Up Phase

Tracking progress and effectiveness of recommendations and remediation plan

Follow-Up Stage

1. Follow-up to determine if control deficiency have been corrected
2. Obtain evidence / re-test control
3. Close the deficiency
4. Monitor effectiveness of corrective actions

Next Steps

Next Steps

1. Course Recommendation
   - IT Audit Complete Course
   - Microsoft Excel – Complete Beginner to Pro Guide
2. IT Audit & Cybersecurity Live Class
3. Start applying for jobs

Certifications

Congratulations !!!