IT Compliances & Security Audits

Presented by Urvi Chheda At The Hacker’s Meetup,Surat

Who Am I

- Certified Ethical Hacker
- Certified Network Defender
- ISO 27001: Lead Auditor
- CISM
- CISSP

in Urvi Chheda

X Urvi

IT Compliance: Ensuring that an organization adheres to legal, regulatory, and internal policies and standards related to information technology.

Key Objectives:

- Protecting sensitive data
- Mitigating risks
- Ensuring legal and regulatory compliance
- Enhancing operational efficiency

Common IT Compliance Frameworks:

- GDPR (General Data Protection Regulation)
- HIPAA (Health Insurance Portability and Accountability Act)
- PCI DSS (Payment Card Industry Data Security Standard)

Security Audits:A systematic evaluation of an organization's information system, security controls, and policies to ensure the protection of data and compliance with regulations.

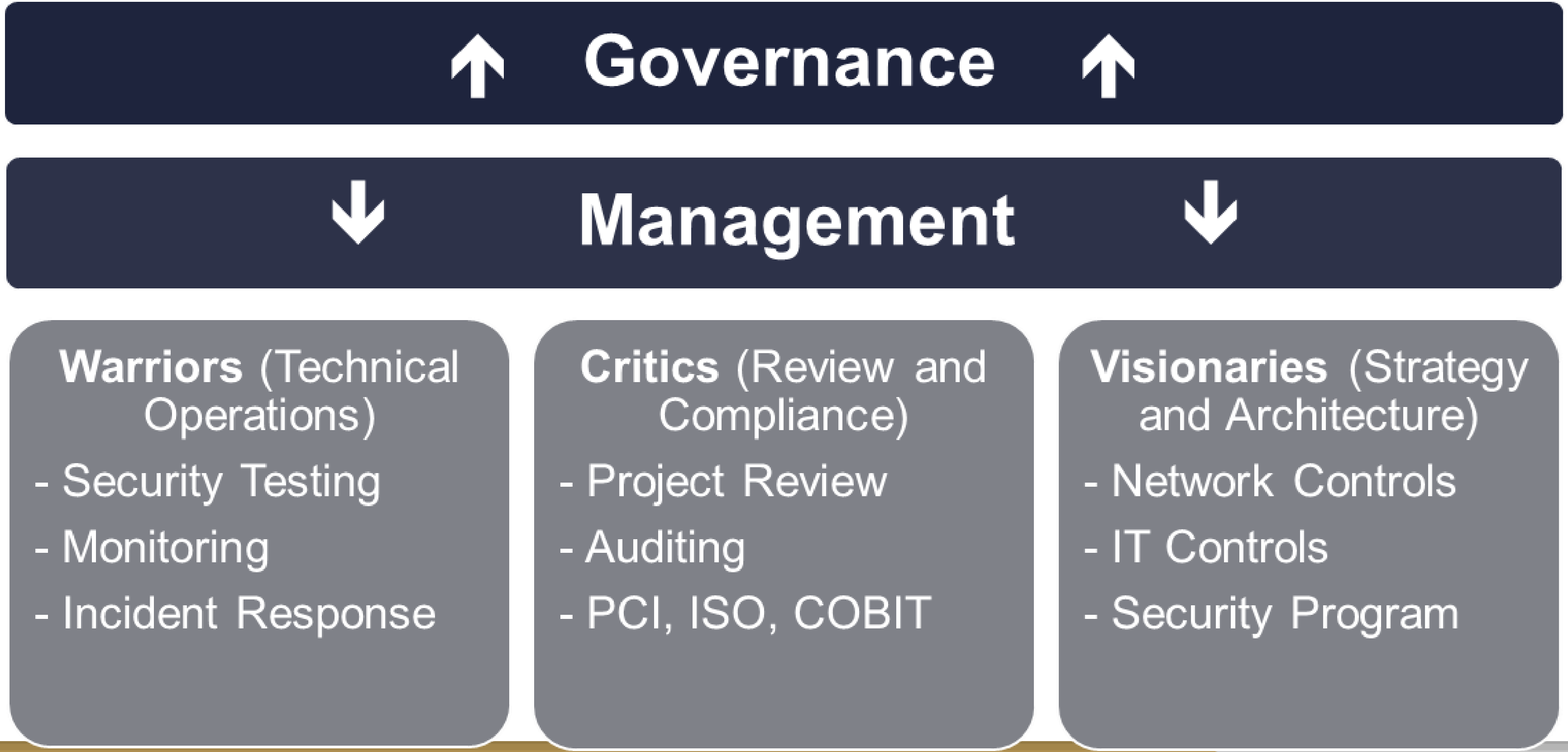
Key Objectives:

- Identifying vulnerabilities
- Ensuring adherence to security policies
- Mitigating risks and threats
- Improving overall security posture

Types of Security Audits:

- **Internal Audits**: Conducted by the organization’s own staff.
- **External Audits**: Conducted by independent third parties.
- **Compliance Audits**: Focused on adherence to regulatory requirements.
- **Vulnerability Assessments**: Identifying and addressing security weaknesses.

The Cyber Security Practice



↑ **Governance** ↑

↓ **Management** ↓

Warriors (Technical Operations)

- Security Testing
- Monitoring
- Incident Response

Critics (Review and Compliance)

- Project Review
- Auditing
- PCI, ISO, COBIT

Visionaries (Strategy and Architecture)

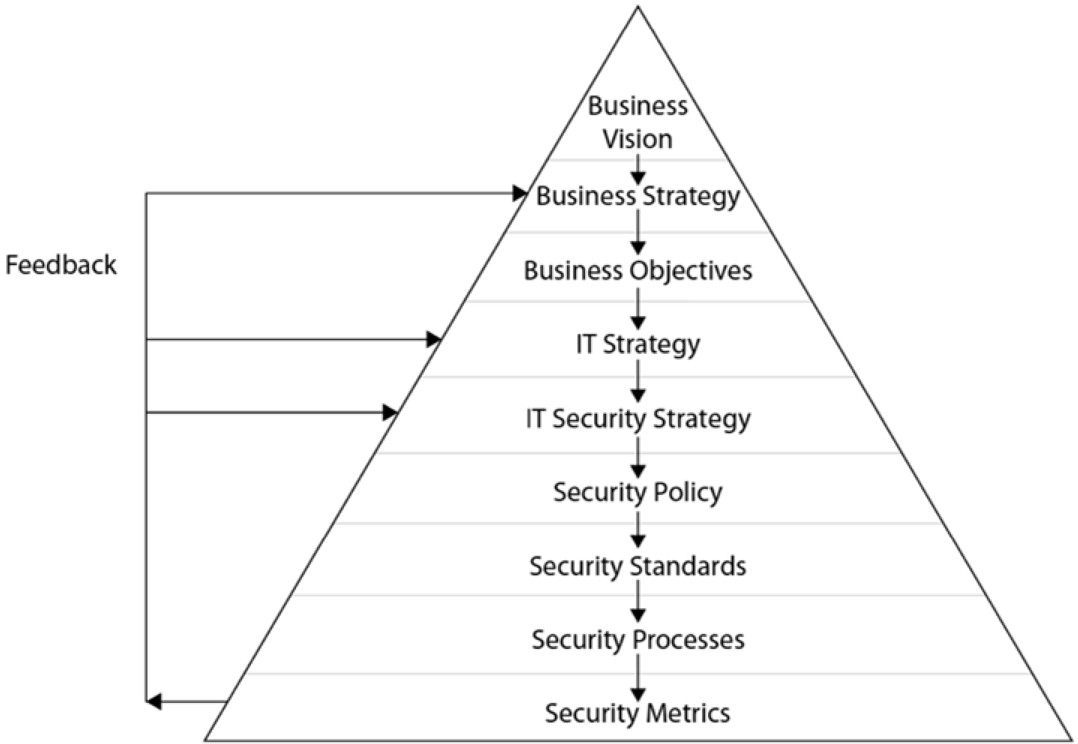
- Network Controls
- IT Controls
- Security Program

Information security governance

Key focus processes:

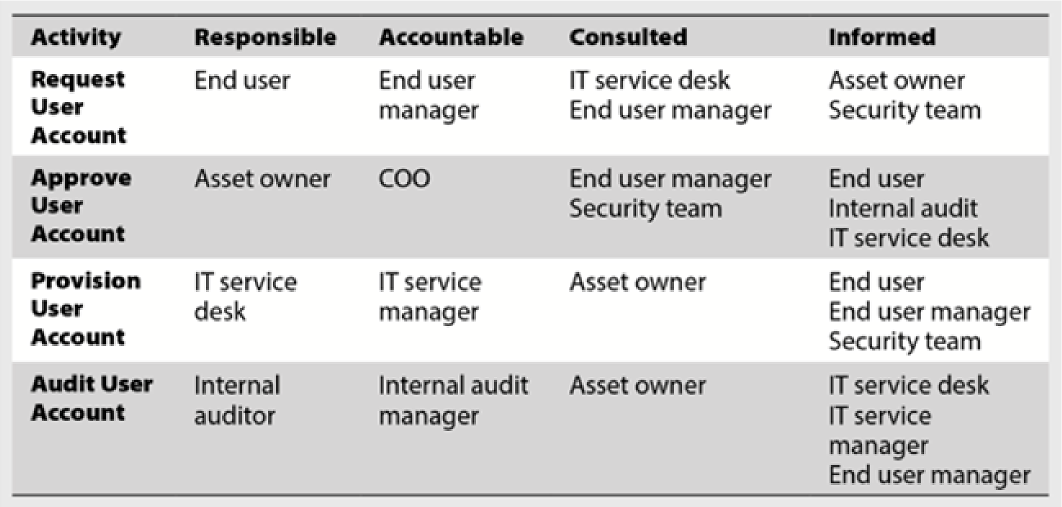
- Personnel management
- Sourcing
- Risk management
- Configuration management
- Change management
- Access management
- Vulnerability management
- Incident management
- Business continuity management

Business vision flows down



Roles and responsibilities

- Security is everyone's responsibility
- There is no business without trusting staff
- Be clear on different roles and their part to play
- RACI charts
  - Responsible
  - Accountable
  - Consulted
  - Informed



Activity	Responsible	Accountable	Consulted	Informed
Request User Account	End user	End user manager	IT service desk End user manager	Asset owner Security team
Approve User Account	Asset owner	COO	End user manager Security team	End user Internal audit IT service desk
Provision User Account	IT service desk	IT service manager	Asset owner	End user End user manager Security team
Audit User Account	Internal auditor	Internal audit manager	Asset owner	IT service desk IT service manager End user manager

Cyber security roles and responsibilities

It can only succeed with leadership commitment

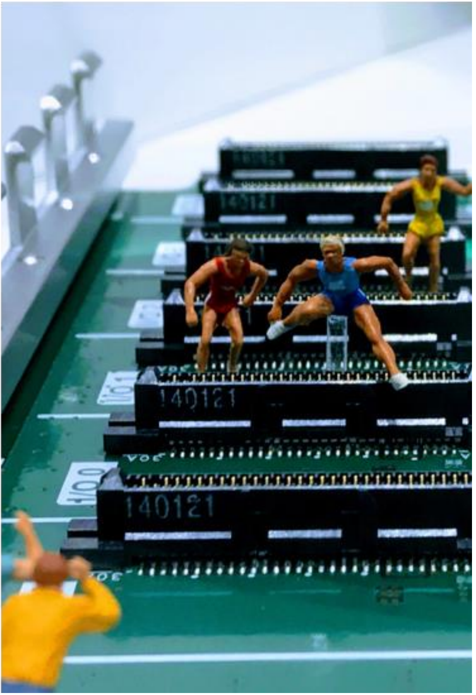
- Obtain clear approval for security strategy and roadmap
- Measure compliance to policies

Establish Reporting and communication channels

- Reporting mapped to endorsed security program
- Implementation progress
- Status of risks and threats
- Compliance level objectives

Information Security Strategy Common Pitfalls

- Overconfidence – in accurate estimates
- Optimism – in forecasts
- Anchoring – on the first presented number
- The *status quo* bias – change reluctance
- Mental accounting – creative money
- The herding instinct – follow the popular idea
- False consensus – over-estimate shared view



Information Security Strategy Resources

Policies – high level statements about behaviour and management intent

Standards – statements about boundaries

Procedures – Operating procedures

Guidelines – Helpful for use with procedures and new technologies

Audit Compliance Findings

Non-compliance Issues:

- **Description**: Identify specific areas of non-compliance.
- **Example**: "The audit revealed missed quarterly risk assessments required by GDPR."

Impact Analysis:

- **Description**: Describe the potential or actual impact.
- **Example**: "Missing assessments could lead to fines and increased data breach risk."

Root Cause:

- **Description**: Identify underlying reasons for non-compliance.
- **Example**: "Inadequate staffing in the compliance department caused the issue."

Recommendations:

- **Description**: Provide actionable steps to address issues.
- **Example**: "Hire more compliance staff and implement automated tracking tools."

Strategy Constraints

- Legal and regulatory
- Record retention
- E-discovery
  - Subpoenas
  - Warrants
- Physical – space and capacity

THANK
YOU