CHAPTER 14

# IT RISK MANAGEMENT & SECURITY

Deep reliance on IT brings risks that can **disrupt operations, compromise data and undermine trust** — from cyberattacks to natural disasters. Covers **risk & its management**, the **components** of IT risk management, **physical, digital, human, environmental, third-party & compliance** risks, the **role of IT security** and future trends.

## CHAPTER ROADMAP

1. Understanding risk — objectives · importance
2. Key components of IT risk mgmt — 6
3. Types of IT risks & mitigation — 6
4. The role of IT security — + future trends

**RISK**

**The possibility of an event or condition that could lead to harm, loss or disruption.**

Inherent in every business; assessed by **probability** (likelihood) and **impact** (degree of harm). IT dependency adds risks beyond traditional concerns.

**RISK MANAGEMENT**

**A systematic process of identifying, assessing and controlling risks to minimise their negative impact.**

Goal: **business continuity**, protect assets, **operational resilience** — turning risk management into a **strategic advantage**.

**Identification** (pinpoint potential risks) › **Assessment** (likelihood × impact (scoring)) › **Mitigation** (reduce · avoid · transfer · accept) › **Monitoring & Review** (track & adapt ↻)

## 1.2 IT RISK MANAGEMENT

*secure · reliable · resilient digital operations*

Focuses on **identifying, assessing and mitigating risks** associated with **IT infrastructure, applications and data** — cybersecurity threats, system outages, data integrity issues.

### Key Objectives

**Protect IT Infrastructure**
Hardware, software, networks from damage, failures, unauthorised access.

**Ensure Data Integrity**
Accuracy, consistency, trustworthiness through the lifecycle.

**Maintain Availability**
Uninterrupted access for operations & customers.

**Mitigate Cyber Threats**
Malware, phishing, **zero-day exploits**.

**Support Compliance**
Legal & industry standards → avoid penalties.

### 1.3 Strategic Importance

**Digital Transformation**
Secure cloud, AI, blockchain, big data → **innovate confidently**.

**Business Continuity**
Operate through attacks, disasters, failures.

**Trust & Compliance**
Align with data laws → credibility.

**Agility & Resilience**
Adapt & **recover quickly**.

**Competitive Advantage**
Reliability & security attract clients.

# 2 KEY COMPONENTS OF IT RISK MANAGEMENT

*structured & methodical*

2.1 Identify › 2.2 Assess › 2.3 Mitigate / Respond › 2.4 Monitor › 2.5 Incident Response › Report & Document

## 2.1 Risk Identification

Foundation — **"you cannot manage what you do not know"**. Sources: cyber threats, physical vulnerabilities, human error, external dependencies.

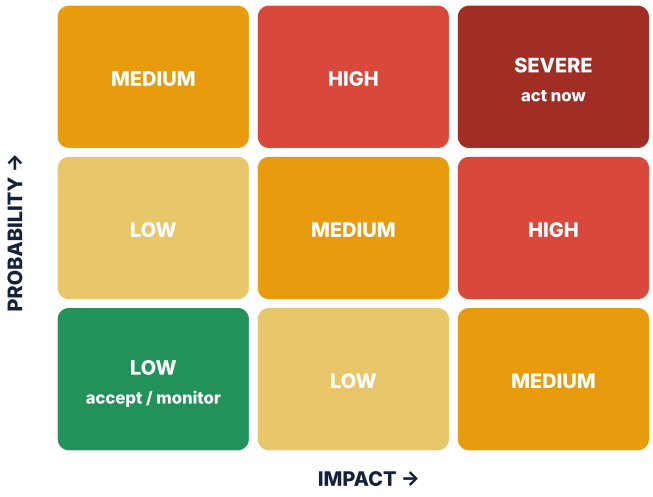
| | |
|---|---|
| **Risk workshops** | Cross-functional teams (IT, finance, HR) give different perspectives |
| **Threat modelling** | Hypothetical models of how an **attacker** could exploit weaknesses |
| **Historical incident analysis** | Review past incidents → recurring risks |

## 2.2 Risk Assessment

Assess **impact & likelihood** to prioritise. Frameworks: **NIST SP 800-30**, **ISO 31000**.

**1. Risk Analysis** nature, sources, vulnerabilities, existing controls › **2. Risk Evaluation** vs criteria: risk appetite, compliance, objectives › **3. Decision** mitigate · transfer · accept · monitor

**Key elements:** Impact analysis · Probability assessment · **Risk matrix**




**Risk matrix** combines **impact × probability** to classify severity.

- **High impact + high probability** — severe → immediate mitigation
- **High-priority risks warrant** — controls/upgrades · transfer · leadership oversight
- **Medium / low** — monitoring plans or accept (document residual risk)

Prioritisation → **optimal use of resources** aligned with strategic goals.

*Matrix drawn as an LL illustration of the study-text description.*

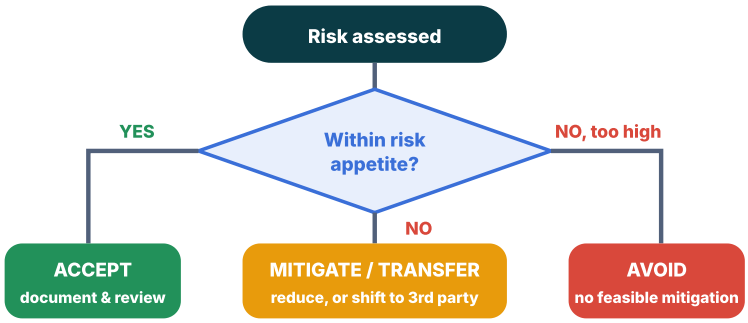
# 2.3 RISK MITIGATION & RESPONSE STRATEGIES

*risk treatment*

**RISK APPETITE**

**The level of risk an organisation is prepared to accept in pursuit of its objectives.**

**Fraud-loss appetite = PKR 10m / year**
Scenario loss **PKR 8m** → within appetite → accept / monitor.
Scenario loss **PKR 25m** → exceeds appetite → mitigate, transfer or avoid.




Simplified LL decision flow based on the study text

## a MITIGATION — reduction

Controls reduce **likelihood or impact** — does **not eliminate** risk; brings it to an acceptable level.

- Patching & updates
- RBAC & **least privilege**
- Security awareness training
- **DRP & BCP**
- Network segmentation & encryption

## b AVOIDANCE — stop the activity

**Eliminate** the risk by avoiding the activity — when risk is too high and no mitigation can bring it within threshold.

Institution **doesn't enter crypto** while regulation is uncertain.

## c TRANSFER — to a third party

Shift the risk via **contractual arrangements**.

**Cyber insurance** for breach losses; **outsourcing** data processing to a more secure provider.

## d ACCEPTANCE — live with it

Low impact & likelihood, and **mitigation costs more than the benefit**. Must be **documented & periodically reviewed**.

Occasional minor glitches in a **non-critical** app.

## 2.4 Risk Monitoring

Continuous surveillance to catch threats **before they escalate**.

- **SIEM** — aggregates & analyses security data in real time
- **Audits & assessments** — compliance; vulnerability assessments
- **Real-time** — IDS, firewalls, **EDR**

## 2.5 Incident Response Plan

Incidents still happen → detect, contain, resolve quickly.

- **Incident classification** — low / medium / high / critical + escalation
- **Communication protocols** — employees, customers, regulators
- **Post-incident review** — root cause, lessons

## Reporting & Documentation

Transparency, accountability, audits, compliance.

- **Incident reports** — knowledge base
- **Risk registers** — risks, assessments, mitigation
- **Compliance records** — GDPR, HIPAA, PCI DSS

# 2.6 SCOPE OF IT RISK MANAGEMENT

**Cybersecurity**
Compromise **confidentiality, integrity, availability**: hacking, phishing & social engineering, malware/ransomware, **DDoS**.

**Physical Infrastructure**
Servers, data centres: natural disasters, theft/vandalism, hardware malfunction, power surges.

**System Failures**
Server crashes, software bugs / unpatched flaws, network outages.

**Human Errors**
Misconfigured firewalls, deleted data, falling for phishing.

## 3 TYPES OF IT RISKS & MITIGATION STRATEGIES

*physical · digital · human · environmental · third-party · compliance*

### 3.1 Physical Risks
tangible IT components

| Sub-type | Detail / case |
|---|---|
| **Natural disasters** | Floods, earthquakes — **Hurricane Sandy 2012** flooded New York data centres |
| **Theft & vandalism** | Stolen laptops/servers |
| **Hardware failures** | Wear, defects, power surges |
| **Power outages** | Grid or internal failures |

**Mitigation:** DRP & BCP with **offsite backups** · physical security (biometrics, CCTV, guards) · **hardware redundancy** & maintenance · **UPS** & generators · **geographic diversification**

### 3.2 Digital Risks
software, networks, data

| Sub-type | Case |
|---|---|
| **Malware & ransomware** | **Colonial Pipeline 2021** — US fuel disrupted |
| **Phishing** | Fake emails/texts steal credentials |
| **Data breaches** | **Equifax 2017** — 147m people, unpatched flaw |
| **DDoS** | **Dyn 2016** — DNS provider; Amazon, Netflix hit |
| **Zero-day exploits** | **SolarWinds 2020** — flaw unknown to vendor |

**Mitigation:** firewalls, **IDPS**, antivirus, patches · training & simulated phishing · **AES-256** encryption · **MFA** · DDoS protection & rate limiting · vulnerability scans & **penetration testing** · incident response plan

## 3.3 Human Risks

"the weakest link"

| | |
|---|---|
| **Negligence & errors** | Misconfigured **Amazon S3** bucket, 2018 |
| **Social engineering** | Phishing, pretexting, baiting |
| **Malicious insiders** | **Tesla 2020** — employee tried to sell data |
| **Lack of awareness** | Weak passwords, oversharing |

**Mitigation:** awareness training · **least privilege** & RBAC · behavioural monitoring (**UEBA**) · policies & audits · simulated attacks · strict **exit procedures** (revoke access)

## 3.4 Environmental Risks

outside direct control

| | |
|---|---|
| **Power outages** | **Venezuela 2019** blackout — banking, healthcare |
| **Climate change** | 2021 Pacific NW heatwave strained cooling |
| **Geopolitical instability** | 2022 sanctions cut Russian access to Western cloud |
| **Pandemics** | COVID-19 remote work → unsecured home networks |

**Mitigation:** UPS, generators, renewables · climate-adapted data centres · diversify vendors / supply chains · secure remote work (**VPN**, endpoint, device policies) · include in BCP

## 3.5 Third-Party Risks

vendors · CSPs · partners

| | |
|---|---|
| **Vendor weaknesses** | **SolarWinds 2020** via software update |
| **Cloud misconfigurations** | 2019 — **540m Facebook** records exposed |
| **Supply chain attacks** | **Kaseya 2021** ransomware to customers |
| **Regulatory non-compliance** | Third party's breach → your penalty |
| **Service interruptions** | **AWS outage 2021** |

**Mitigation:** vendor risk assessments & SLAs · **TPRM** tools · cloud configuration standards · **SBOM** · contractual safeguards · backup providers

## 3.6 Compliance & Regulatory Risks

fines · legal · reputation

**Pakistan:** SBP ETGRMF · SECP Cyber Security Guidelines · **PECA 2016** · Cyber Security Policy · **ETO 2002**

**IMF & FATF:** FATF sets **AML / CFT** & proliferation-financing standards; IMF checks via **FSAPs**. Pakistan has been on and off the **FATF grey list** → less FDI, higher cross-border costs, scrutiny.

**Tech for compliance: RegTech** (AI/NLP track rule changes) · **AML/CFT** ML anomaly detection, risk-based KYC · digital forensics & automated audit trails · **blockchain/DLT** immutable records

| Risk type | Potential impact | Key mitigation |
|---|---|---|
| **Physical** | Downtime, data loss, hardware damage | DRP, physical security, redundancy, power backup |
| **Digital** | Breaches, financial loss, outages | Firewalls, antivirus, encryption, MFA, DDoS protection |
| **Human** | Data exposure, vulnerabilities | Training, access controls, monitoring, simulated attacks |
| **Environmental** | Disruption, cost increases | Power resilience, climate adaptation, remote security |
| **Third-party** | Breaches, outages, compliance issues | Vendor assessments, monitoring, contracts |
| **Compliance** | Fines, legal action, restrictions | RegTech, automated reporting, AML/CFT systems |

# 4 THE ROLE OF IT SECURITY

*defence-in-depth*

A **critical pillar** of IT risk management. Adopt **defence-in-depth** — **layering multiple security controls** to reduce vulnerabilities across a wide spectrum of threats.

## 4.1.1 Access Controls

### RBAC vs ABAC

**RBAC** — by **job role**, consistent. **ABAC** — by **attributes** (department, location, time) — dynamic, context-aware.

### Least Privilege

**Minimum access** needed → smaller attack surface.

### MFA

Something you **know** (password), **have** (OTP, smart card), **are** (biometrics).

### PIM — Privileged Identity Mgmt

Identify, manage & audit **privileged identities** (admin/service accounts).

- **Just-in-time (JIT)** access
- Auto-expiry of elevated rights
- Monitoring & alerts

Microsoft Entra ID PIM · CyberArk · BeyondTrust

### PAM — Privileged Access Mgmt

Control & monitor what privileged users **do** on critical systems.

- **Credential vaulting**
- **Session recording** & audit
- Command filtering

Thycotic Secret Server · One Identity Safeguard · CyberArk PSM

### Identity Governance (IGA)

Integrate PIM & PAM with IGA → consistent policy, **compliance reporting**, identity lifecycle.

SailPoint · IBM Security Verify · Oracle Identity Governance

## 4.1.2 Encryption Controls

**AES-256**
256-bit key; almost impossible to crack. For data **at rest** & **in transit**. *A digital vault with a secret code.*

**PKI**
**Two keys** (encrypt / decrypt) + **digital certificates** (online ID). Protects **https**, email, digital signatures.

## 4.1.3 Incident Response — 6 steps

1. **Preparation**
2. **Detection**
3. **Analysis**
4. **Containment** — stop spread
5. **Eradication** — remove threat
6. **Recovery**

**SIEM** = "security camera & control room" — collects logs, alerts on odd activity (e.g., midnight login from abroad).

### 4.2 Advanced Technologies

- **AI & ML** — threat intelligence, anomaly detection, automated threat hunting; faster than rule-based
- **Zero Trust** — no implicit trust, continuous verification, **micro-segmentation**
- **Blockchain** — immutable audit trails, digital identity

### 4.3.1 Hardware Controls

- **HSM** — protects cryptographic keys & signatures in tamper-resistant hardware
- **TPM** — platform integrity, **secure boot**, key storage
- Physical — biometric locks, surveillance, restricted zones

### 4.3.2 Network Controls

- **Next-gen firewalls**
- **IDS/IPS** — detect / block
- **VPNs** — secure remote access
- **Segmentation** — limits **lateral movement**

### 4.3.3 Endpoint Security

- Antivirus / antimalware
- **EDR** — real-time detection & forensics
- **MDM** — secure devices accessing corporate data

### 4.4 Policy & Governance

- Acceptable use, password & data-classification policies
- Frameworks: **ISO/IEC 27001, NIST CSF, COBIT**
- Continuous compliance (GDPR, HIPAA, SBP); automated tools

### 4.5 Security in Architecture

- **Secure SDLC** — testing at every phase
- **DevSecOps** — security in the CI/CD pipeline
- **CSPM** — finds cloud misconfigurations

**KEY IDEA** Security should be **built into enterprise architecture**, not treated as an afterthought.

## 4.6 FUTURE TRENDS IN IT RISK MANAGEMENT

**Increased Automation**
AI/ML for real-time detection & response; less manual work.

**Climate-Related Risks**
Floods, fires, extreme weather damaging data centres.

**Global Regulatory Changes**
Stricter privacy & security laws worldwide.

**Cyber-Physical Integration**
IoT & smart grids — secure digital **and** physical parts.

## EXAM FOCUS · MCQ TRAPS

*commonly confused points*

**1 Mitigation ≠ elimination**
Mitigation **reduces** to an acceptable level; **avoidance** eliminates by stopping the activity.

**2 Transfer examples**
Cyber insurance and outsourcing = **transfer**, not mitigation.

**3 Acceptance rule**
Only when low impact/likelihood and control cost > benefit — must be **documented & reviewed**.

**4 Assessment phases**
Analysis → **Evaluation** (vs risk appetite) → Decision.

**5 Threat modelling**
An **identification** technique — thinking like an attacker.

**6 PIM vs PAM**
PIM manages privileged **identities** (JIT, expiry). PAM controls privileged **access/sessions** (vaulting, recording).

**7 RBAC vs ABAC**
RBAC = role. ABAC = attributes like **location & time**.

**8 IR order**
Containment (stop spread) comes **before** eradication (remove threat).

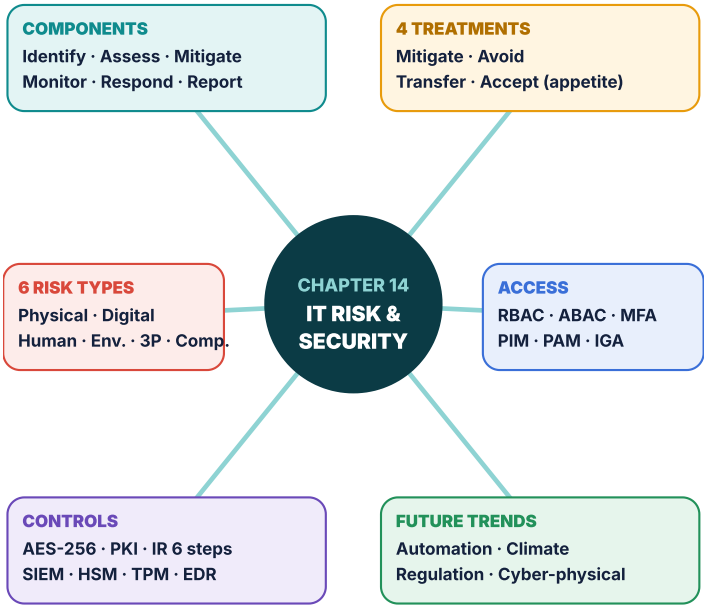
**9 HSM vs TPM**
HSM = protect **keys/signatures**. TPM = **secure boot** & platform integrity.

**10 Case → risk type**
SolarWinds = zero-day / third-party · Equifax = breach · Tesla = insider · Venezuela = environmental.

## CLASSIFY IT

| | | |
|---|---|---|
| 1 | Buy cyber insurance | Transfer |
| 2 | Skip crypto market entirely | Avoidance |
| 3 | Patch systems monthly | Mitigation |
| 4 | Live with minor app glitches | Acceptance |
| 5 | Hurricane floods data centre | Physical risk |
| 6 | Vendor's update spreads malware | Third-party risk |
| 7 | Access allowed only 9–5 from office | ABAC |
| 8 | Admin sessions recorded | PAM |

## REVISION MAP




**Risk**
Probability × impact of harm, loss or disruption.

**Process**
Identify → assess → treat → monitor → respond.

**Treat**
Mitigate, avoid, transfer or accept vs appetite.

**Types**
Physical, digital, human, environmental, 3rd-party, compliance.

**Secure**
Defence-in-depth: access, encryption, IR, zero trust.