CHAPTER 16

IT GENERAL CONTROLS FOR MANAGING RISK

IT General Controls (ITGCs) are policies, procedures and practices that ensure the **integrity, confidentiality and availability** of the IT environment. Covers their **objectives**, **importance**, the **5 key components**, a **5-step implementation** process and the **challenges** of managing them.

CHAPTER ROADMAP

1 Introduction to ITGCs
2 Key objectives 4
3 Importance 6
4 Key components 5
5 Implementing ITGCs 5 steps
6 Challenges 5

DEFINITION

ITGCs are the foundational processes, policies and procedures that ensure the integrity, reliability and security of an organisation's IT systems.

They are **broad-based** — they apply to **all aspects** of the IT infrastructure. Help prevent unauthorised access, data breaches and system failures.

IT GENERAL CONTROLS
Broad framework covering the **whole IT environment** — reliability & security of all systems

vs

APPLICATION CONTROLS
Tailored to individual software systems — specific to one application

2 KEY OBJECTIVES OF ITGCS

4 · interconnected

Ensure Data Integrity

Prevent unauthorised **access, modification or deletion**; access restrictions, validation, **audit trails**.

Failure → wrong financial reports, penalties.

Maintain Availability

Systems up when needed — **redundancy, disaster recovery**, maintenance.

Simulated **failover tests**.

Safeguard Confidentiality

Stop unauthorised **disclosure** — encryption, access controls, training.

e.g. **zero-trust** architecture.

Support Compliance

Align with **ISO 27001, SOX**, local data laws — audits, documentation, policy enforcement.

New rules for AI & blockchain.

3 IMPORTANCE OF ITGCS

Risk Mitigation
First line of defence — standardised processes reduce vulnerabilities.

Financial Accountability
Reliable data for reporting — required under **SOX**.

Operational Continuity
Availability for supply chain & customer service.

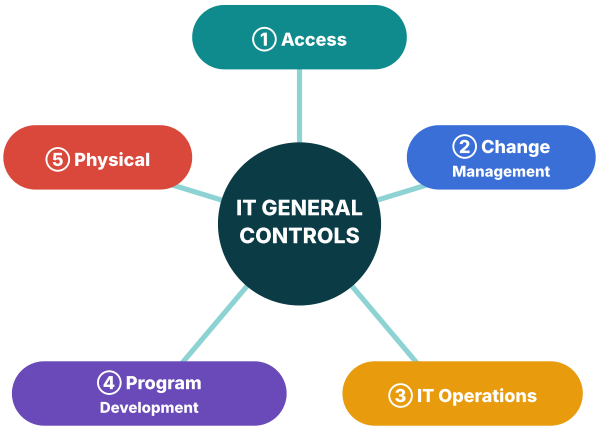
Trust & Reputation
Protects sensitive data & privacy.

Adaptability
Integrate AI, IoT, **quantum computing** securely.

Regulatory & Legal Protection
Avoid fines & legal action.

4 KEY COMPONENTS OF ITGCS

5 · together form the control environment



MEMORY HOOK

"A Clever IT Person Protects" → **A**ccess · **C**hange management · **IT** operations · **P**rogram development · **P**hysical security.

4.1 Access Controls

who can get in

Restrict unauthorised access to systems, apps & data.

User authentication	Passwords, **MFA**, biometrics — *bank: password + mobile OTP*
RBAC	Access by **job role** — *finance can't open HR systems*
PAM	Restrict & monitor **admins**; log, time-limit, separate accounts — *hospital patient data*

4.2 Change Management

planned · authorised · tested

Uncontrolled changes → disruption, vulnerabilities, failures.

Change approval	Formal approval — *CRM upgrade approved by IT manager & head of sales*
Testing & validation	Unit, integration, **UAT** before production — *payment gateway in a **sandbox***
Documentation	Why, who approved, test results — ***change log** for auditors*

4.3 IT Operations

day-to-day running

Keep systems secure, available, performing.

Backup & recovery	Daily **offsite** backups; **test restores** quarterly
Incident management	Identify, report, resolve fast — *telecom restores in minutes*
System monitoring	Alerts before escalation — *handle holiday traffic spikes*

4.4 Program Development

secure new software

No vulnerabilities introduced during development; meets requirements.

Requirement analysis	Define business & technical needs first
Code reviews	**Peer review** finds security flaws early
Testing	Unit, integration, **UAT** with end users

4.5 Physical Security

tangible IT assets

Protect servers, data centres, devices from physical threats.

Access control	Key cards, **biometrics**, guards; entry logs
Environmental	Fire suppression, temperature control, **UPS**, generators
Surveillance	**CCTV**, alarms, motion sensors

Spot the component

- "Who **can log in**?" → **Access**
- "Was the **update approved & tested**?" → **Change mgmt**
- "Can we **restore / keep running**?" → **IT operations**
- "Is the **new app** built safely?" → **Program development**
- "Can someone **walk into** the server room?" → **Physical**

5 IMPLEMENTING IT GENERAL CONTROLS

5 steps · aligned with risk framework

① Risk Assessment › ② Control Design › ③ Implementation › ④ Training & Awareness › ⑤ Monitoring & Review ↻

① Risk Assessment

- **Identify risks** — cyber, physical, human, compliance
- **Analyse vulnerabilities** — outdated software, no encryption, unpatched systems
- **Assess impact** — financial, reputational, operational

Output → a **risk register** prioritised by likelihood & impact.

② Control Design

Select control types:

- **Preventive — access controls**
- **Detective — monitoring**
- **Corrective — backup & recovery**

- **Align** with business (e-commerce → uptime; bank → confidentiality)
- **Cost-benefit analysis**

③ Implementation

- **Deploy controls** — configure systems, permissions, monitoring tools
- **Change management** — authorise, test, document
- **System integration** — **pilot testing** before full roll-out

④ Training & Awareness

- **Employee training** on role-specific controls
- **Awareness campaigns** — phishing simulations, reminders
- **Stakeholder engagement** — vendors & partners comply

⑤ Monitoring & Review

- **Real-time monitoring** — SIEM
- **Regular audits** & assessments
- **Continuous improvement**
- **Incident reporting & feedback**

Control types — quick check

Preventive	Stops it happening
Detective	Spots it happening
Corrective	Fixes it afterwards

6 CHALLENGES IN MANAGING ITGCS

6.1 Complex IT Environments

Cloud, on-premise, mobile, IoT; **legacy systems** lack modern security; fast tech change (AI, blockchain).

6.2 Resource Constraints

Budget limits · scarce **expertise** · **overburdened** IT teams.

6.3 Evolving Threats

APTs, ransomware, phishing, zero-days; AI used by attackers; more frequent attacks.

6.4 Regulatory Changes

Changing rules · **cross-jurisdiction** differences · stricter penalties.

6.5 Flexibility vs Security

User resistance (MFA) → workarounds · **performance** trade-offs · business agility.

BALANCE Overly **rigid** controls stifle innovation; overly **lax** controls expose risk — take a **proactive, adaptive** approach.

EXAM FOCUS · MCQ TRAPS

commonly confused points

1 General vs application controls
ITGCs = **broad**, whole IT environment. Application controls = **one specific system**.

2 5 components
Access · Change management · IT operations · Program development · Physical security.

3 Where's backup?
Backup & recovery sits under **IT operations** controls — and is a **corrective** control type.

4 UAT appears twice
Under **change management** (testing changes) and **program development** (testing new software).

5 Code reviews
A **program development** control — peer review to catch flaws early.

6 UPS & fire suppression
Environmental controls within physical security.

7 Step order
Assess → Design → Implement → Train → Monitor. Risk register comes from **step 1**.

8 Cost-benefit
Done at **control design** — the control's cost must be justified by the risk mitigated.

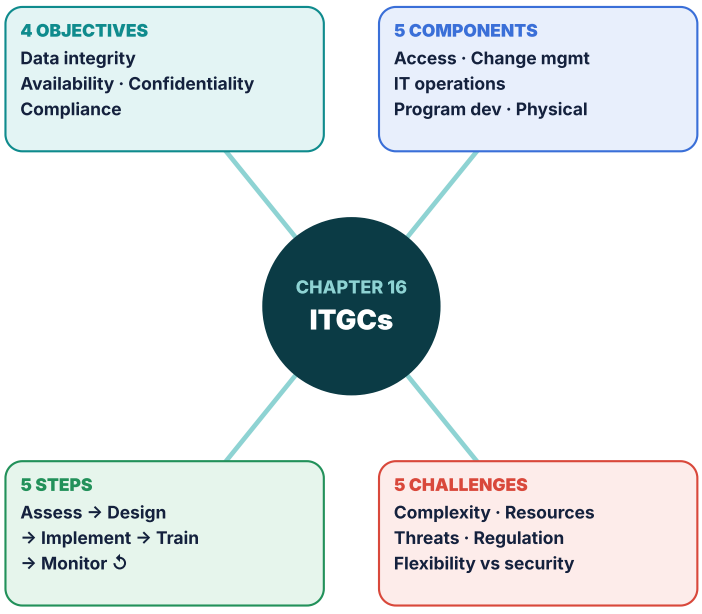
9 SOX
Links ITGCs to **financial reporting reliability**.

10 User resistance
A **flexibility vs security** challenge — leads to workarounds.

CLASSIFY IT

1	Admin access logged & time-limited	Access (PAM)
2	New gateway tested in sandbox	Change mgmt
3	Quarterly restore test	IT operations
4	Peer review of fintech code	Program dev.
5	Biometric entry to data centre	Physical
6	SIEM flags anomaly	Detective
7	Staff bypass MFA	Flex vs security
8	Prioritised list of IT risks	Risk register

REVISION MAP



ITGCs
Broad controls over the whole IT environment.

Aim
Integrity, availability, confidentiality, compliance.

Components
Access, change, operations, development, physical.

Implement
Assess, design, deploy, train, monitor.

Challenges
Complexity, resources, threats, rules, balance.