CHAPTER 17

ICT'S ROLE IN RISK MANAGEMENT

Organisations face growing **cyber, operational, compliance, financial and strategic** risks. **Information & Communication Technology (ICT)** provides the tools, systems and insights to **identify**, **report** and **mitigate** them — plus **7 best practices** for integrating ICT into risk management.

CHAPTER ROADMAP

1	Risk mgmt in modern organisations	5 risk areas
2	ICT in risk identification	4
3	ICT in risk reporting	4
4	ICT in risk mgmt & mitigation	4
5	Best practices for integrating ICT	7

Risk management now goes **far beyond traditional approaches**, driven by **globalisation, digital transformation, regulatory complexity** and the rising importance of **corporate governance**. **ICT plays a dual role**: it **introduces new risks** (e.g., cyberattacks) **and** provides the **tools to manage them**.

1 KEY RISK AREAS & HOW ICT HELPS

5 categories

1.1 Cybersecurity
attack surface ↑ (cloud, mobile, IoT)

- **Data breaches** — customer, financial, IP data; GDPR pressure
- **Ransomware** — now targets whole supply chains
- **Phishing & social engineering** — human entry point
- **Insider threats** — hard to detect

1.2 Operational
day-to-day processes

- **System failures** — banking, manufacturing, healthcare
- **Supply chain disruptions** — ICT monitors in real time, finds alternatives
- **Process inefficiencies** — automation, ERP, **process mining**

ICT: real-time monitoring, predictive maintenance, automation.

1.3 Compliance
laws & standards

- **Regulatory violations** — fines, legal battles
- **Legal penalties** — environmental, labour, financial-reporting rules

ICT: track rule changes, automate checks; **GRC platforms** (governance, risk & compliance).

1.4 Financial
loss of assets / profit

- **Fraud** — identity theft, payment fraud, insider trading → AI pattern recognition, blockchain
- **Market volatility** → big data & predictive analytics to hedge
- **Economic downturns** → forecasting tools

1.5 Strategic
long-term decisions

- **Poor decision-making** → analytics & **BI platforms**
- **Technological obsolescence** → infrastructure for cloud, AI, blockchain
- **Competitive threats** → monitor competitors

Remember the five

C	Cybersecurity
O	Operational
C	Compliance
F	Financial
S	Strategic

2 · IDENTIFY find risks early › **3 · REPORT** inform stakeholders › **4 · MANAGE & MITIGATE** reduce & respond

2 ICT'S ROLE IN RISK IDENTIFICATION

first phase of risk management

① DATA ANALYTICS & MONITORING
AI / ML spot unusual patterns

Collects data from **transaction logs, network traffic, IoT, social media**. ML learns **normal behaviour** and flags deviations.

e.g. AI detects unusual logins or abnormal transactions → fraud / breach.

② REAL-TIME MONITORING
continuous watch

Up-to-date insight so threats don't go unnoticed. Tools: **IDS** and **SIEM** — gather data, analyse logs, flag abnormal activity.

e.g. SIEM sends real-time alerts on unauthorised data access.

③ PREDICTIVE MODELLING
history → future risk

Data mining, statistical models, ML on historical data forecast recurring risks.

e.g. Supply-chain tools anticipate disruption from geopolitics, economy, disasters.

④ AUTOMATED RISK SCANNERS
find weaknesses

Vulnerability scanners & **penetration testing** simulate attacks; find gaps, unpatched software, misconfigurations; recommend fixes.

e.g. Network scans reveal misconfigured firewalls & old patches.

3 ICT'S ROLE IN RISK REPORTING

executives · managers · regulators

① DASHBOARDS & VISUALISATION
risk at a glance

Aggregate data into **charts, graphs, heat maps** — risk metrics, incident status, mitigation progress.

e.g. Cyber dashboard: phishing attempts, vulnerabilities, resolved incidents.

② AUTOMATED REPORTING
no manual effort

Scheduled reports from templates, sent to executives, **audit committees**, regulators.

e.g. Bank reports **KRIs** — capital adequacy, liquidity — to management.

③ CENTRALISED RISK REPOSITORIES
one source of truth

Cloud-based platform storing all risk data → consistency, transparency, collaboration.

e.g. MNC's regional teams log risks → **unified global view**.

④ REGULATORY COMPLIANCE TOOLS
prove adherence

Track rule changes, auto-generate compliance reports, keep **audit trails**.

e.g. Banking compliance software submits reports automatically.

4 ICT'S ROLE IN RISK MANAGEMENT & MITIGATION

Risk Mitigation Tools

Encryption, firewalls, IPS, antivirus — protect assets, cut exposure.

e.g. Encrypting customer data on bank servers.

Incident Response Systems

Predefined, often **automated** protocols: **isolate** threats, shut down systems, notify.

e.g. Malware found → machine disconnected automatically.

Business Continuity & DR

Backups, **redundant networks**, cloud storage; cloud DR **replicates offsite**.

e.g. Restore after a data-centre outage.

Automated Risk Control

Self-healing networks & intelligent threat detection — act **without manual intervention**.

e.g. Traffic rerouted from a failing server.

5 BEST PRACTICES FOR INTEGRATING ICT INTO RISK MANAGEMENT

7

Practice	How ICT helps	Example / extra strategies
① **Adopt a proactive approach**	Predictive analytics, real-time monitoring, AI detection → **anticipate**, not just react	Predict raw-material shortages; **scenario planning**; AI **early-warning** systems
② **Ensure data accuracy & integrity**	Validation, quality checks, **audit trails**	Validate transaction data to avoid anti-fraud **false positives**; data governance; **blockchain** records
③ **Foster collaboration across teams**	Collaboration platforms, cloud, unified risk software	**Cross-functional risk committees** (finance, IT, compliance); Teams/Slack; co-authoring & version control
④ **Regularly update & test systems**	Automated updates, **patch management**, security testing	Regular **penetration testing**; quarterly / biannual system audits
⑤ **Train employees on ICT tools**	**Learning management systems (LMS)**, role-specific modules, simulations	Cyber awareness; **mock phishing**; certifications & incentives
⑥ **Leverage automation**	Real-time monitoring, alerts, auto-reports, preventive actions	Automated vulnerability scanners; automated reporting; **RPA** for data entry & compliance checks
⑦ **Continuously improve**	Feedback loops, **post-incident analysis** refine models	Review policies; **benchmark** against industry standards; track control effectiveness

MEMORY HOOK **"People Don't Collaborate Unless Trained, Automated, Improved"** → **P**roactive · **D**ata integrity · **C**ollaboration · **U**pdate & test · **T**rain · **A**utomate · **I**mprove.

EXAM FOCUS · MCQ TRAPS

commonly confused points

1 ICT's dual role
ICT both **creates** new risks and **provides tools** to manage them.

2 Identify vs report
SIEM / IDS / scanners = **identification**. Dashboards / KRI reports / repositories = **reporting**.

3 Predictive modelling
Uses **historical** data to forecast — an identification tool.

4 Penetration testing
Appears as an **automated risk scanner** (identify) and in **update & test** (best practice).

5 KRIs
Key risk indicators (capital adequacy, liquidity) — sent via **automated reporting**.

6 Self-healing network
An **automated risk control system** (mitigation) — reroutes traffic.

7 GRC platforms
Support **compliance** risk management.

8 Obsolescence
Falling behind on technology is a **strategic** risk, not operational.

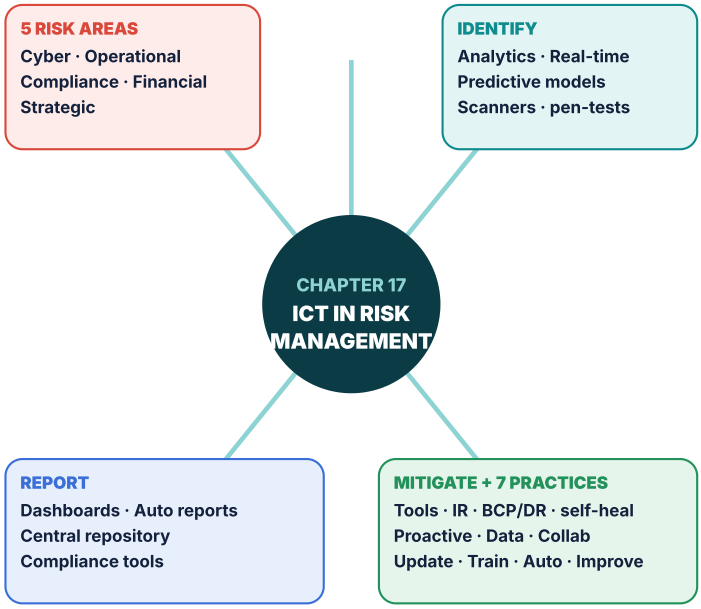
9 Process mining
ICT tool for **operational** process inefficiencies.

10 LMS
Supports the **train employees** best practice.

CLASSIFY IT

1	Heat map of open incidents	Reporting
2	ML flags a 3 a.m. login	Identification
3	Infected PC auto-isolated	Mitigation (IR)
4	Regional teams log in one cloud system	Central repository
5	Rival launches disruptive product	Strategic risk
6	Insider trading	Financial (fraud)
7	Mock phishing campaign	Train employees
8	RPA does compliance checks	Leverage automation

REVISION MAP



Risks
Cyber, operational, compliance, financial, strategic.

Identify
Analytics, monitoring, prediction, scanners.

Report
Dashboards, auto reports, repositories, compliance.

Mitigate
Tools, IR, BCP/DR, self-healing.

Integrate
7 best practices — proactive to continuous.