ISO/IEC 27002:2022 – Control Groups (Learning Summary)

This resource provides an overview of the **four control groups** in ISO/IEC 27002:2022.
It gives short explanations so students can understand the purpose of each type of control without needing the full paid standard.

---

1. Organisational Controls (37 controls)

These set the direction for information security and define how security is managed across the organisation.

Key Areas with Short Explanations

- **Policies and governance**
  High-level direction for security and clear expectations for behaviour and responsibilities.
- **Roles and responsibilities**
  Defines who is accountable for decisions, approvals and day-to-day actions.
- **Risk management processes**
  Provides a structured approach to identifying, assessing and treating risks.
- **Supplier and third-party management**
  Ensures external partners meet required security standards.
- **Project and change management**
  Makes sure new systems and changes include security from the start.
- **Access control rules**
  Sets principles for how access is granted, reviewed and removed.
- **Logging and monitoring strategy**
  Defines what needs to be logged and how activity is monitored for unusual behaviour.
- **Backup strategy**
  Sets expectations for creating, storing and verifying backups.
- **Cryptographic management**
  Ensures encryption and key handling follow approved practice.
- **Incident management structure**
  Defines roles, responsibilities and steps to respond to incidents.
- **Business continuity planning**
  Provides a high-level framework for maintaining security during disruption.

---

2. People Controls (8 controls)

These address human behaviour, awareness and the way individuals access information.

Key Areas with Short Explanations

- **Screening and onboarding**
  Ensures staff are suitable and trusted before gaining access.
- **Security awareness and training**
  Teaches staff how to recognise and avoid security threats.
- **Disciplinary processes**
  Supports consistent handling of security breaches by staff.
- **Offboarding and role changes**
  Ensures access is removed or adjusted when people leave or change duties.

---

3. Physical Controls (14 controls)

These protect physical environments, equipment and locations.

Key Areas with Short Explanations

- **Secure areas**
  Restricts entry to sensitive rooms and facilities.
- **Physical entry controls**
  Uses locks, cards, logs and monitoring to protect access.
- **Equipment protection**
  Prevents loss, theft or damage of devices and infrastructure.
- **Environmental controls**
  Reduces risks from fire, flood, power issues or temperature changes.
- **Clear desk and clear screen**
  Prevents exposure of information in shared or open spaces.

---

4. Technological Controls (34 controls)

These are implemented through technology to protect systems, networks and data.

Key Areas with Short Explanations

- **User authentication**
  Ensures users prove their identity before accessing systems.
- **Access control mechanisms**
  Manages permissions within applications and systems.

- **Endpoint protection**
  Defends laptops, servers and mobile devices against malware or exploitation.
- **Configuration management**
  Applies secure settings and baselines to systems.
- **Network security**
  Uses segmentation, filtering and secure communication methods.
- **Logging and monitoring tools**
  Collects and analyses events to detect unusual activity.
- **Backup implementation**
  Runs, tests and restores backups to ensure data recovery.
- **Encryption and key handling**
  Protects data using secure cryptographic methods.
- **Change management in systems**
  Ensures updates and changes are controlled and reviewed.
- **System hardening**
  Reduces attack surface by disabling unnecessary features or services.
- **Vulnerability management**
  Identifies and addresses weaknesses in systems and software.

How to Use This Resource

You can use this list to:

- Explain control groups in their own words
- Complete ISMS and Annex A-related tasks
- Justify control selection in a Statement of Applicability
- Map controls to frameworks like NIST CSF or CIS Controls
- Support assignment work without needing the paid standards
