ISO/IEC 27001:2022 – Annex A Controls (Complete List)

A.5 – Organizational Controls (37 Controls)

A.5.1 Policies for information security

A.5.2 Information security roles and responsibilities

A.5.3 Segregation of duties

A.5.4 Management responsibilities

A.5.5 Contact with authorities

A.5.6 Contact with special interest groups

A.5.7 Threat intelligence

A.5.8 Information security in project management

A.5.9 Inventory of information and assets

A.5.10 Acceptable use of information and assets

A.5.11 Return of assets

A.5.12 Classification of information

A.5.13 Labelling of information

A.5.14 Information transfer

A.5.15 Access control

A.5.16 Identity management

A.5.17 Authentication information

A.5.18 Access rights

A.5.19 Information security in supplier relationships

A.5.20 Addressing information security in supplier agreements

A.5.21 Managing security in the ICT supply chain

A.5.22 Monitoring and review of supplier services

A.5.23 Information security for use of cloud services

A.5.24 Information security incident management responsibilities

A.5.25 Reporting information security incidents

A.5.26 Assessment of information security events

A.5.27 Response to information security incidents

A.5.28 Learning from incidents

A.5.29 Collection of evidence

A.5.30 Information security continuity

A.5.31 ICT readiness for business continuity

A.5.32 Legal and regulatory requirements

A.5.33 Intellectual property rights

A.5.34 Protection of PII

A.5.35 Independent review of information security

A.5.36 Compliance with policies and standards

A.5.37 Documented operating procedures

A.6 – People Controls (8 Controls)

A.6.1 Screening

A.6.2 Terms of employment

A.6.3 Security awareness and training

A.6.4 Disciplinary process

A.6.5 Responsibilities after termination

A.6.6 Non-disclosure agreements

A.6.7 Remote working

A.6.8 Teleworking

A.7 – Physical Controls (14 Controls)

A.7.1 Physical security perimeters

A.7.2 Physical entry control

A.7.3 Securing offices and facilities

A.7.4 Security monitoring

A.7.5 Protection against environmental threats

A.7.6 Working in secure areas

A.7.7 Clear desk and screen

A.7.8 Equipment protection

A.7.9 Assets off-premises

A.7.10 Media disposal

A.7.11 Supporting utilities

A.7.12 Cabling security

A.7.13 Equipment maintenance

A.7.14 Equipment reuse and disposal

A.8 – Technological Controls (34 Controls)

A.8.1 Secure development lifecycle

A.8.2 Change management

A.8.3 Information deletion

A.8.4 Data masking

A.8.5 Data leakage prevention

A.8.6 Monitoring activities

A.8.7 Clock synchronization

A.8.8 Use of privileged utilities

A.8.9 Configuration management

A.8.10 Capacity management

A.8.11 Protection against malware

A.8.12 Backup

A.8.13 Logging

A.8.14 Monitoring

A.8.15 Technical vulnerabilities control

A.8.16 Vulnerability management

A.8.17 System audit considerations

A.8.18 Secure coding

A.8.19 Secure authentication

A.8.20 Cryptographic controls

A.8.21 Key management

A.8.22 Network security

A.8.23 Network segregation

A.8.24 Web filtering

A.8.25 Application security

A.8.26 Secure configuration

A.8.27 Operations security

A.8.28 Technical compliance review

A.8.29 Vulnerability scanning

A.8.30 Patch management

A.8.31 Security testing

A.8.32 Source code review

A.8.33 Endpoint security

A.8.34 Email security