ISO 27001

CONTROLS MADE EASY

MAKING INFOSEC RELATABLE THROUGH SCHOOL SCENARIOS!

PART 3

Control Number	Control Name	Real Life Example	Implementation Guidance
8.1	**User end point devices**	Schools manage various devices used by teachers and students - laptops for teaching, tablets for digital learning, desktop computers in labs. Like having rules for using school equipment, each device has specific usage guidelines and protection measures. **Information Security Connection:** Organizations must secure all user devices accessing corporate information. Like schools protecting educational devices, companies need to secure laptops, phones, and tablets with proper controls to protect company data accessed or stored on these devices002E	• Create device usage policies • Implement security controls • Configure device protection • Monitor device usage • Manage device updates • Control data access • Document issued devices • Regular security reviews
8.2	**Privileged access rights**	Schools restrict special access rights - only IT teachers can install software, only administrators can access student records system, only exam coordinators can access question paper storage. Like having master keys limited to specific staff, special access is carefully controlled. **Information Security Connection:** Organizations must strictly control privileged system access. Like schools limiting administrative access, companies need to carefully manage who gets elevated system rights, ensuring only authorized personnel can perform sensitive system operations.	• Identify privileged access needs • Document approval process • Limit privileged accounts • Monitor privileged activities • Regular access reviews • Log special access usage • Revoke unused privileges • Audit privilege changes

8.3	**Information access restriction**	Schools restrict access to different information - teachers see only their class records, counsellors access only their student files, finance staff see only accounting data. Like having different keys for different rooms, information access is based on need. **Information Security Connection:** Organizations must restrict information access based on business needs. Like schools controlling access to student records, companies need to limit who can access specific information through proper access controls and authentication.	• Define access rules • Implement access controls • Document access rights • Review access regularly • Monitor information usage • Handle access violations • Update access rules • Maintain access logs
8.4	**Access to source code**	Schools protect their custom software - like student management systems or exam result calculators. Only authorized IT staff can modify these programs, with changes tracked like how textbook revisions are controlled. Like keeping master copies of exam papers secure, source code needs special protection. **Information Security Connection:** Organizations must protect program source code. Like schools securing their custom applications, companies need to control who can access and modify software code to prevent unauthorized changes and protect intellectual property.	• Secure code repositories • Control developer access • Track code changes • Review code modifications • Backup source code • Monitor code access • Document code versions • Audit code controls
8.5	**Secure authentication**	Schools use various methods to verify identity - ID cards for physical access, passwords for computer login, signatures for important documents. Like checking parent ID during student pickup, proper	• Define authentication requirements • Implement strong verification • Manage authentication methods

		verification ensures only authorized access. **Information Security Connection:** Organizations must implement strong authentication methods. Like schools verifying identity before access, companies need reliable ways to confirm user identity before allowing system access, using methods like passwords, biometrics, or security tokens.	• Monitor login attempts • Handle failed attempts • Train users on security • Review authentication effectiveness • Update security measures
8.6	**Capacity management**	Schools manage their resources capacity - ensuring enough classrooms for students, adequate computer lab stations, sufficient internet bandwidth for online classes. Like planning classroom size for expected students, resources are monitored and adjusted based on needs. **Information Security Connection:** Organizations must manage IT resource capacity. Like schools ensuring adequate facilities, companies need to monitor and manage system resources (storage, processing, bandwidth) to prevent failures or performance issues that could impact security.	• Monitor resource usage • Plan capacity needs • Set performance alerts • Regular capacity reviews • Handle resource issues • Document capacity plans • Forecast future needs • Update resources timely
8.7	**Protection against malware**	Schools protect their computers from harmful programs - like installing antivirus software, checking USB drives, filtering internet access. Like having health checks to prevent disease spread, schools take measures to keep their systems healthy.	• Install protection software • Keep definitions updated • Scan systems regularly • Monitor system behaviour • Respond to alerts • Train users on threats

		Information Security Connection: Organizations must protect against malicious software. Like schools protecting school computers, companies need comprehensive malware protection including antivirus, web filtering, and email scanning to prevent system infections.	• Document incidents • Review protection effectiveness
8.8	**Management of technical vulnerabilities**	Schools regularly check and fix safety issues - repairing broken windows, fixing loose electrical connections, maintaining playground equipment. Like regular health check-ups identify potential problems early, schools constantly look for and fix safety risks. **Information Security Connection:** Organizations must identify and fix system vulnerabilities. Like schools maintaining safe facilities, companies need to regularly scan for technical weaknesses in their systems and applications, applying necessary fixes to prevent security breaches.	• Regular vulnerability scans • Prioritize identified issues • Apply security patches • Test system updates • Monitor fix effectiveness • Track vulnerable assets • Document remediation • Review scanning process
8.9	**Configuration management**	Schools maintain standard setups - classroom layouts, computer settings, laboratory equipment arrangements. Like having a standard way to arrange library books, proper configuration ensures everything works consistently and safely. **Information Security Connection:** Organizations must maintain secure system configurations. Like schools standardizing classroom setups, companies need standard security settings	• Define secure configurations • Document standard settings • Control configuration changes • Regular configuration checks • Track system settings • Update standards • Monitor compliance • Maintain configuration records

		for systems and devices, ensuring they're configured securely and consistently.	
8.10	**Information deletion**	Schools properly remove old information - shredding old exam papers, wiping computers before disposal, securely disposing of student records after retention period. Like clearing lockers at year-end, all outdated or unnecessary information is properly removed. **Information Security Connection:** Organizations must securely delete information when no longer needed. Like schools properly disposing of old records, companies need procedures to permanently remove sensitive data from systems and storage devices to prevent unauthorized recovery.	• Create deletion procedures • Use secure deletion methods • Verify data removal • Track deletion activities • Handle storage media • Document data removal • Train staff on procedures • Audit deletion process
8.11	**Data masking**	Schools hide sensitive details when sharing information - using student IDs instead of names on public lists, covering grades when displaying work, showing only necessary information in reports. Like using initials instead of full names, sensitive data is carefully masked. **Information Security Connection:** Organizations must protect sensitive data through masking. Like schools hiding student details, companies need to conceal sensitive information when used in non-production environments or shared with unauthorized parties.	• Identify sensitive data • Define masking rules • Implement masking tools • Test masked data • Control access to original data • Monitor masking effectiveness • Document procedures • Review masking methods
8.12	**Data leakage prevention**	Schools prevent unauthorized information sharing - controlling what files can be copied to USB	• Identify sensitive data flows • Implement monitoring tools

		drives, monitoring email attachments, restricting photo-taking in certain areas. Like having rules about sharing class photos on social media, schools control how information leaves the school. **Information Security Connection:** Organizations must prevent unauthorized data exposure. Like schools controlling information sharing, companies need systems to detect and prevent sensitive data from leaving through email, web, or portable devices.	• Set prevention rules • Monitor data movement • Handle violations • Train users on policies • Document incidents • Review effectiveness
8.13	**Information backup**	Schools maintain copies of important information - duplicating student records, backing up digital files, keeping spare copies of important documents. Like having backup answer sheets during exams, critical information is always duplicated for safety. **Information Security Connection:** Organizations must regularly backup information. Like schools keeping copies of important records, companies need systematic backup procedures to prevent data loss and ensure business continuity.	• Define backup requirements • Implement backup systems • Test recovery process • Secure backup storage • Monitor backup success • Document backup schedule • Regular recovery tests • Review backup strategy
8.14	**Redundancy of information processing facilities**	Schools maintain backup facilities - multiple computer labs, spare projectors, alternative internet connections. Like having backup generators for power cuts or spare bells for announcements, critical systems have fallback options to keep school running.	• Identify critical systems • Create redundant setups • Test failover process • Maintain backup systems • Monitor system health • Document procedures

		Information Security Connection: Organizations must have redundant systems for critical operations. Like schools having backup facilities, companies need duplicate systems and equipment to ensure business continues even if primary systems fail.	• Regular testing • Review effectiveness
8.15	**Logging**	Schools keep various activity records - visitor logs, library book checkouts, computer lab usage times. Like maintaining attendance registers, all important activities are recorded for tracking and review. **Information Security Connection:** Organizations must record system and user activities. Like schools tracking various activities, companies need comprehensive logging of system access, security events, and user actions for security monitoring and investigations.	• Define logging requirements • Configure system logs • Protect log information • Regular log reviews • Set retention periods • Monitor log storage • Handle log alerts • Document findings
8.16	**Monitoring activities**	Schools monitor various activities - teachers supervising playgrounds, CCTV watching corridors, staff monitoring computer usage. Like watching students during exam time, continuous monitoring helps detect and prevent problems early. **Information Security Connection:** Organizations must actively monitor security-related activities. Like schools watching for unusual behaviour, companies need to monitor systems and networks for suspicious activities, security events, and potential threats.	• Set monitoring scope • Deploy monitoring tools • Define alert thresholds • Train monitoring staff • Handle security alerts • Document incidents • Regular reviews • Update monitoring rules

8.17	**Clock synchronization**	Schools ensure all clocks show the same time - classroom clocks, bell system, biometric attendance machines. Like coordinating exam timings across classrooms, synchronized time ensures activities run smoothly and records are accurate. **Information Security Connection:** Organizations must synchronize all system clocks. Like schools coordinating time across campus, companies need all systems to have the same time for accurate logging, monitoring, and incident investigation.	• Set time source standards • Configure system clocks • Monitor synchronization • Handle time drift • Document time zones • Regular checks • Maintain accuracy • Review effectiveness
8.18	**Use of privileged utility programs**	Schools restrict powerful tools - only IT staff can use system configuration tools, only lab technicians can access specialized lab equipment controls, only admin staff can use school database utilities. Like keeping master keys secure, powerful tools need special control. **Information Security Connection:** Organizations must control use of powerful system utilities. Like schools restricting access to specialized tools, companies need to strictly control who can use administrative utilities that could bypass system security controls.	• Identify powerful utilities • Restrict access rights • Monitor utility usage • Document approved users • Control installation • Log all usage • Regular access review • Remove unnecessary tools
8.19	**Installation of software on operational systems**	Schools control software installation - only approved educational apps on school tablets, only licensed software on lab computers, only IT department can install programs. Like controlling what books enter the library, software	• Create installation policy • Define approved software • Control installation rights • Test before installation

		installation follows strict rules. **Information Security Connection:** Organizations must control software installation. Like schools managing educational software, companies need procedures to ensure only approved and secure software is installed on operational systems.	• Document all changes • Monitor compliance • Remove unauthorized software • Regular software audits
8.20	**Networks security**	Schools protect their networks - separate Wi-Fi for staff and guests, firewalls for internet safety, secured admin networks. Like having different corridors for different grade students, networks are separated and protected based on their use. **Information Security Connection:** Organizations must secure all networks. Like schools protecting their Wi-Fi networks, companies need comprehensive network security including firewalls, segmentation, and monitoring to protect against unauthorized access and cyber threats.	• Design secure networks • Implement protection tools • Monitor network traffic • Control network access • Regular security updates • Document network layout • Test security controls • Review effectiveness
8.21	**Security of network services**	Schools manage different network services - internet for learning, specialized software for administration, online portals for parents. Like having different buses for different routes, each service has specific security requirements and controls. **Information Security Connection:** Organizations must secure all network services. Like schools protecting their online services, companies need to secure network services through proper	• Define service requirements • Implement security controls • Monitor service levels • Manage service providers • Document agreements • Regular service reviews • Handle service issues • Update security measures

		controls, monitoring, and service level agreements with providers.	
8.22	**Segregation of networks**	Schools separate different networks - administrative network for staff, learning network for students, guest network for visitors. Like having separate entrances for students and visitors, different networks are kept apart for better security. **Information Security Connection:** Organizations must separate different network types. Like schools having different networks for different users, companies need to segregate networks based on security requirements and business needs.	• Identify network types • Plan network separation • Implement segregation • Control traffic flow • Monitor segments • Document network design • Regular reviews • Test separation
8.23	**Web filtering**	Schools filter internet access - blocking inappropriate websites, controlling social media access, protecting students from harmful content. Like having a librarian guide student to appropriate books, web filtering ensures safe internet usage. **Information Security Connection:** Organizations must filter web access. Like schools protecting students online, companies need web filtering to protect against malicious websites, data leakage, and inappropriate content access.	• Define filtering rules • Implement web filters • Create allowed/blocked lists • Monitor web access • Handle filter alerts • Update filter rules • Document exceptions • Review effectiveness
8.24	**Use of cryptography**	Schools protect sensitive information through encryption - securing online exam papers, protecting digital student records, safeguarding financial data. Like using sealed envelopes for confidential letters,	• Define encryption needs • Select encryption methods • Manage encryption keys • Train users appropriately

		encryption keeps information secure. **Information Security Connection:** Organizations must use encryption to protect sensitive data. Like schools securing confidential information, companies need encryption for protecting data storage, transmission, and sensitive communications.	• Monitor encryption use • Regular key updates • Document procedures • Review effectiveness
8.25	**Secure development life cycle**	Schools plan new systems carefully - from designing new student portals to implementing grading systems. Like planning a new building with safety in mind, new systems are developed with security built in from the start. **Information Security Connection:** Organizations must integrate security in system development. Like schools planning secure educational systems, companies need to include security throughout the development lifecycle of new systems and applications.	• Define security requirements • Include security in design • Secure coding practices • Regular security testing • Document development • Review security measures • Manage changes securely • Monitor compliance
8.26	**Application security requirements**	Schools specify security needs for applications - secure login for grade systems, data protection for student records, controlled access for library systems. Like setting safety rules for science experiments, every application needs clear security requirements. **Information Security Connection:** Organizations must define security requirements for applications. Like schools securing educational applications, companies need clear security	• Document security needs • Define access requirements • Specify data protection • Set validation rules • Include audit features • Plan error handling • Review requirements • Update as needed

		specifications for all applications to protect data and functionality.	
8.27	**Secure system architecture and engineering principles**	Schools design systems thoughtfully - like planning buildings with emergency exits, proper ventilation and secure entry points. Every school system, from library management to attendance tracking, follows secure design principles. **Information Security Connection:** Organizations must follow secure design principles. Like schools planning safe facilities, companies need to design systems with built-in security features following established security architecture principles.	• Define security principles • Design secure architecture • Document design decisions • Review security plans • Test design effectiveness • Update architecture • Monitor compliance • Regular reviews
8.28	**Secure coding**	Schools ensure quality in creation - like having standards for teaching materials, lesson plans, and assessment papers. Teachers follow proven methods and peer review to ensure quality and accuracy of their work. **Information Security Connection:** Organizations must implement secure coding practices. Like schools ensuring quality in teaching materials, companies need standards and practices for writing secure code to prevent security vulnerabilities.	• Establish coding standards • Train developers properly • Implement code reviews • Use secure components • Test code security • Document practices • Monitor compliance • Update standards regularly
8.29	**Security testing in development and acceptance**	Schools test everything before use - new teaching methods are piloted, new equipment is tested, new procedures are trailed. Like checking playground equipment before student use, all systems need thorough testing.	• Define testing requirements • Create test scenarios • Conduct security testing • Document test results • Fix identified issues

		Information Security Connection: Organizations must test security during development. Like schools testing new methods, companies need comprehensive security testing of systems before deployment to ensure they're secure.	• Verify fixes work • Maintain test records • Review test process
8.30	**Outsourced development**	Schools manage external contractors - like hiring experts to develop custom teaching software or creating the school website. Just as schools ensure quality when outsourcing yearbook printing, they maintain standards for external developers. **Information Security Connection:** Organizations must manage security in outsourced development. Like schools controlling external contractors, companies need to ensure external developers follow security requirements and standards.	• Define security requirements • Include security in contracts • Monitor development work • Review code quality • Test delivered systems • Control source code • Document arrangements • Verify compliance
8.31	**Separation of development, test and production environments**	Schools separate different activities - practice exams in classrooms, mock tests in halls, final exams in dedicated centres. Like having separate areas for rehearsals and actual performances, different activities need different spaces. **Information Security Connection:** Organizations must separate different system environments. Like schools separating practice from real exams, companies need distinct environments for development, testing, and	• Create separate environments • Control access to each • Protect production data • Manage data transfers • Document separation • Monitor environment usage • Regular environment reviews • Maintain separation

		live systems to prevent issues.	
8.32	**Change management**	Schools manage changes systematically - like introducing new teaching methods, updating school policies, or changing classroom technology. Each change follows a process: planning, approval, testing, and implementation, like how curriculum changes are carefully managed. **Information Security Connection:** Organizations must control system changes. Like schools managing educational changes, companies need formal processes for making system changes to prevent disruptions and security issues.	• Create change procedures • Document change requests • Test proposed changes • Get proper approvals • Plan implementations • Monitor change impacts • Keep change records • Review effectiveness
8.33	**Test information**	Schools protect test resources - using sample papers for practice, dummy data for training new teachers, test environments for new systems. Like using practice materials instead of actual exam papers, test information is carefully managed. **Information Security Connection:** Organizations must properly manage test data. Like schools using sample materials, companies need to protect test information and avoid using real production data in test environments.	• Create test data policy • Generate safe test data • Protect test environments • Control test access • Monitor test usage • Delete after testing • Document procedures • Regular reviews
8.34	**Protection of information systems during audit testing**	Schools protect systems during inspections - like education board reviews, safety audits, or system checks. Just as regular classes continue during school inspections, normal	• Plan audit activities • Control audit access • Monitor audit impact

		operations must continue safely during audits. **Information Security Connection:** Organizations must protect systems during audit testing. Like schools managing inspections, companies need to ensure audit activities don't disrupt operations or compromise security.	• Protect live systems • Schedule testing properly • Document audit activities • Review audit effects • Maintain operations

DID YOU FIND THIS CHECKLIST USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

WWW.MINISTRYOFSECURITY.CO