ISO 27001

CONTROLS MADE EASY

MAKING INFOSEC RELATABLE THROUGH SCHOOL SCENARIOS!

PART 1

Control Number	Control Name	Real Life Example	Implementation Guidance
5.1	**Policies for information security**	Think about a school's rule system. They have a main handbook with core rules (like student conduct, safety, or attendance policies) that everyone must follow. Then, they have specific policy sets for different activities - for lab safety rules, library policies, computer usage guidelines, and exam regulations. Just as these rules are reviewed and updated each year based on new needs (like adding online class rules during pandemic), and communicated to all students, teachers, and parents through orientations and circulars. **Information Security Connection:** Organizations need a similar structured approach to security policies. Like schools having a main handbook and specific rules, companies need a main security policy supported by detailed topic-specific policies (like password rules, data handling, network security). These policies must be approved by management, communicated clearly to all employees, and updated regularly to address new threats or business changes.	• Create Information Security Policy aligned with business objectives and requirements • Develop topic-specific policies for key areas (access control, password management, etc.) • Ensure policies include clear objectives, scope, roles and responsibilities • Establish policy management processes including regular reviews Document and maintain policy acknowledgments and changes Communicate policies effectively using clear language and awareness sessions
5.2	**Information security roles and responsibilities**	In a school, each role has specific security responsibilities. The Principal oversees overall security, Department Heads protect teaching materials, IT Teacher manages computer security, and Administrative staff secures student records. Like how a School Counsellor knows they must keep student discussions confidential, each person understands their role in protecting school information. **Information Security Connection:** Just as schools clearly define who's responsible for different aspects of	• Create security organization structure (CISO, Security Managers, Operations teams) • Define responsibilities for each role (decisions, access rights, reporting lines) • Document and communicate through job descriptions and policies • Provide role-specific training and verify

		student information protection, organizations need clearly defined security roles. Like how a School Counsellor knows they must protect student conversations, each person in an organization must understand their role in protecting company data, customer information, and system security.	competency • Review roles annually and update as needed
5.3	**Segregation of duties**	Think about a school's examination process. The Subject Teacher creates the exam, Department Head reviews it, Exam Officer handles secure storage, different teachers supervise the exam, and another group grades it. Similarly, for fee collection - one person collects, another records, and a third verifies. This separation prevents any single person from having too much control. **Information Security Connection:** Like how schools divide exam handling responsibilities, organizations must separate critical IT and security tasks. For example, one person shouldn't be able to both create and approve system changes, or both assign and review access rights, reducing risks of fraud or mistakes.	• Identify critical activities needing separation (financial, admin, security tasks) • Define who can request, approve, and implement changes • Document segregation rules and workflows • Implement role-based access controls • Monitor compliance and review effectiveness
5.4	**Management responsibilities**	The School Principal and Management ensure security measures are followed - like staff background checks, visitor sign-ins, and proper handling of student records. They provide necessary resources (like secure cabinets), ensure staff training, and monitor compliance with security rules. **Information Security Connection:** Similarly, organization's management must actively support information security by ensuring proper resources, enforcing policies, and creating a security-aware culture. Just as a Principal is ultimately responsible	• Define management's security oversight responsibilities • Ensure staff security briefing and training • Enforce policy compliance and handle violations • Provide resources for security implementation • Review security performance regularly

		for student safety, management is accountable for data protection.	
5.5	**Contact with authorities**	Schools maintain relationships with local authorities for different situations - police for security incidents, fire department for safety checks, education board for compliance. The school knows exactly who to contact in each situation, like calling police for suspicious activity or education board for data breach incidents. **Information Security Connection:** Organizations must maintain similar relationships with cybersecurity authorities, regulators, and law enforcement. Like schools reporting serious incidents, organizations need clear procedures for reporting data breaches or cyber attacks to relevant authorities.	• Identify and document relevant authority contacts • Establish incident reporting procedures • Define scenarios requiring authority contact • Maintain current contact information • Test communication channels periodically
5.6	**Contact with special interest groups**	Schools are part of educational networks where they share and learn best practices. For instance, participating in district school meetings to discuss common challenges like handling student data privacy or securing online classes. **Information Security Connection:** Organizations should join cybersecurity forums and industry groups to stay informed about new threats and security practices. Like schools learning from other schools, organizations benefit from shared security knowledge and experiences.	• Join relevant security forums and groups Participate in information sharing platforms • Maintain active membership and engagement • Document and share received information • Review value of memberships annually
5.7	**Threat intelligence**	Schools gather information about potential risks from various sources - local police updates about area safety, weather alerts for school closure, cyber threat alerts for online learning platforms. This helps them prepare and respond appropriately.	• Set up threat intelligence collection process • Subscribe to trusted intelligence sources • Analyse and validate gathered intelligence • Share actionable intelligence internally

		Information Security Connection: Organizations need to gather and analyze cybersecurity threat intelligence from various sources. Like schools preparing for different threats, organizations use this intelligence to protect against potential cyber attacks and security risks.	• Implement protective measures based on threats
5.8	**Information security in project management**	When a school plans new initiatives like an online grade portal or digital library, security is considered from the start. Just as they plan access control and supervision for a new computer lab, they ensure proper security measures are built into every new project from the beginning. **Information Security Connection:** Organizations must integrate security in all projects from inception. Like schools planning security for new facilities, security requirements must be considered when developing new systems or processes, not added as an afterthought.	• Include security requirements in project planning • Conduct security risk assessments • Assign security expertise to projects • Review security at project milestones • Document security implementation decisions
5.9	**Inventory of information and other associated assets**	Schools maintain detailed records of their important assets - from student records to teaching materials, computers to confidential documents. Each item is tracked with details of who's responsible for it, where it's kept, and how sensitive it is. **Information Security Connection:** Organizations must maintain inventory of all information assets. Like schools tracking sensitive student records, companies need to know what information they have, where it's stored, and who's responsible for protecting it.	• Create and maintain asset inventory • Assign ownership for each asset • Classify assets by importance/sensitivity • Update inventory regularly • Track asset location and status
5.10	**Acceptable use of information**	Schools have clear rules for using resources - how to use the computer lab, handle student records, or access the school	• Create acceptable use policy • Define allowed and prohibited activities

	and other associated assets	database. These rules specify what's allowed and what's not, ensuring everyone uses school resources properly. **Information Security Connection:** Organizations need clear policies on how information and systems should be used. Like school computer lab rules, these policies ensure employees understand proper handling of company information and IT resources.	• Communicate guidelines clearly • Monitor usage compliance • Review and update guidelines periodically
5.11	**Return of assets**	When teachers or staff leave the school, they must return all items - laptops, textbooks, keys, ID cards, and student files. A checklist ensures nothing is missed, just like students clearing all dues before getting transfer certificates. **Information Security Connection:** Organizations must ensure all company assets are returned when employees leave. Like schools recovering resources, companies must protect their information assets through proper returns.	• Create asset return checklist for exits • Document all assigned assets per employee • Establish formal return procedures • Verify returned assets condition • Update asset inventory after returns
5.12	**Classification of information**	Schools classify information based on sensitivity - public information (school events), internal use (teaching materials), confidential (student records, exam papers), and strictly confidential (student counseling records). **Information Security Connection:** Organizations must classify information to ensure appropriate protection. Like schools protecting sensitive student data differently from public announcements, companies need different security levels for different types of information.	• Establish classification levels (e.g., Public, Internal, Confidential) • Define criteria for each level • Train staff on classification process • Review and update classifications regularly • Document classification decisions
5.13	**Labelling of information**	Schools use clear labelling to protect different documents - exam papers marked "Confidential", health records labelled "Medical Confidential", announcements	• Create standardized labelling system • Define labelling methods for different formats

		marked "Public", and draft reports labelled "Internal Draft". This helps staff quickly understand how to handle each document, whether it needs secure storage or can be shared openly. **Information Security Connection:** Organizations need similar labelling to ensure proper information handling. Like schools, companies must help employees quickly identify sensitive information and understand handling requirements through clear labels.	• Implement automated labelling where possible • Train users on labelling requirements • Audit labelling compliance
5.14	**Information transfer**	Schools have specific procedures for information sharing - student records are transferred between schools in sealed envelopes, exam papers move in locked bags, and confidential emails are encrypted. From sending report cards to parents to sharing student performance with education boards, each type of information has defined transfer methods. **Information Security Connection:** Organizations must establish secure information transfer methods based on sensitivity levels. Like schools protecting student records during transfers, organizations need secure protocols for both physical and digital information sharing. This includes encryption, transfer agreements, and monitoring to ensure information remains protected throughout its journey.	• Define secure transfer methods • Establish transfer agreements • Implement encryption for sensitive transfers • Document chain of custody • Monitor transfer compliance
5.15	**Access control**	A school carefully controls access - teachers can only access their class records, counsellors have exclusive access to student counselling files, and exam papers are accessible only to authorized staff. Each staff member has specific access rights based on their role and responsibilities. **Information Security Connection:**	• Create access control policy • Implement role-based access • Document access approval process • Regular access reviews • Monitor access patterns

		Organizations must implement comprehensive access control based on job roles and need-to-know basis. Like schools restricting teachers' access to only their class records, companies need technical controls to limit system and data access. This includes proper authentication, regular access reviews, and the principle of least privilege.	
5.16	**Identity management**	Schools maintain unique IDs for all staff and students - each person has their own login for the school system, unique ID cards, and specific credentials. When someone leaves, their IDs are deactivated, just as new joiners get their unique identifiers. **Information Security Connection:** Organizations need robust identity management systems to uniquely identify users across all systems. Like schools managing student and staff IDs, companies must maintain unique identifiers, manage the complete identity lifecycle from creation to deletion, and ensure proper authentication methods.	• Establish unique identifier system • Define identity verification process • Maintain identity lifecycle • Handle shared accounts securely • Regular identity reviews
5.17	**Authentication information**	Schools manage authentication carefully - staff have unique passwords for grade systems, secure ID cards for physical access, and special codes for sensitive areas like exam rooms. These credentials are regularly updated and securely managed. **Information Security Connection:** Organizations must securely manage all authentication credentials. Like schools protecting access to sensitive areas, companies need strong password policies, secure credential management, and regular updates to authentication methods to prevent unauthorized access.	• Define strong authentication requirements • Secure credential distribution process • Implement password management systems • Handle reset procedures securely • Regular authentication review

5.18	**Access rights**	In schools, access rights vary by role - principals can access all records, teachers see only their class information, and administrative staff have limited access to student records. These rights change when roles change, like when a teacher becomes a department head. **Information Security Connection:** Organizations must implement role-based access rights with regular reviews and updates. Like schools adjusting access when teachers change roles, companies need processes to modify access rights as employees change positions, ensuring access remains appropriate to job functions.	• Document access rights process • Link rights to job roles • Regular rights review • Handle role changes • Maintain access records
5.19	**Information security in supplier relationships**	Schools ensure security with external partners - bus services protecting student route information, cafeteria vendors maintaining food allergy records confidentially, and software providers securing online learning platforms. **Information Security Connection:** Organizations must manage security risks from supplier relationships. Like schools ensuring vendors protect student information, companies need to assess supplier security capabilities, include security requirements in contracts, and regularly monitor compliance.	• Define supplier security requirements • Assess supplier security capabilities • Include security in contracts • Monitor supplier compliance • Regular security reviews
5.20	**Addressing information security within supplier agreements**	Schools have detailed agreements with suppliers - specifying how educational software companies handle student data, how security companies protect school premises, and how maintenance staff access restricted areas. **Information Security Connection:** Organizations must clearly define security requirements in supplier contracts. Like schools establishing data protection rules with	• Document security requirements • Include incident reporting procedures • Define security responsibilities • Specify compliance requirements • Include right to audit

		educational software providers, companies need detailed security clauses in vendor agreements, including incident reporting and compliance requirements.	
5.21	**Managing information security in the information and communication technology (ICT) supply chain**	Schools verify security across their technology chain - from educational software providers to computer suppliers to network service providers. Each component's security is assessed and monitored to protect student information. **Information Security Connection:** Organizations must manage security across their entire ICT supply chain. Like schools ensuring all technology components are secure, companies need to verify security at each supply chain level, from software components to hardware suppliers to service providers.	• Map complete ICT supply chain • Define security requirements for suppliers • Regular security assessments • Monitor component security • Implement vulnerability management
5.22	**Monitoring, review and change management of supplier services**	Schools regularly monitor their service providers - checking if online learning platforms are secure, reviewing security camera maintenance, and ensuring school bus tracking systems protect student data. When providers make changes, schools assess security impact. **Information Security Connection:** Organizations must continuously monitor supplier service security. Like schools reviewing educational service providers, companies need to assess service changes, monitor security performance, and ensure continued compliance with security requirements.	• Establish clear monitoring metrics and reporting schedules • Conduct regular supplier security assessments and compliance checks • Create and maintain change management procedures for supplier services • Document and track all security incidents and resolutions • Hold regular performance review meetings with key suppliers • Maintain updated inventory of all supplier services and their security requirements • Develop escalation procedures for security issues • Review supplier access rights and permissions regularly

5.23	**Information security for use of cloud services**	Schools carefully manage cloud services used for online learning, student records, and administrative tasks. They ensure data is protected, access is controlled, and backup procedures are in place, just like protecting physical student records. **Information Security Connection:** Organizations must implement proper security controls for cloud services. Like schools protecting student data in cloud platforms, companies need strong access controls, data protection measures, and clear procedures for data handling in cloud environments.	• Assess security capabilities of cloud providers • Define data protection requirements for cloud services • Implement access controls and monitoring • Establish backup and recovery procedures • Create cloud service exit strategy • Monitor cloud service security performance • Document cloud security responsibilities • Train users on secure cloud usage
5.24	**Information security incident management planning and preparation**	Schools have clear plans for handling security incidents - from lost student records to unauthorized access of grade systems. Everyone knows their role, reporting procedures, and required actions, just like fire drill procedures. **Information Security Connection:** Organizations need structured incident response plans. Like schools handling security breaches, companies must have clear procedures, defined roles, and trained teams to manage security incidents effectively.	• Create incident response plan and procedures • Define incident response team and roles • Establish incident reporting mechanisms • Develop incident classification system • Set up communication procedures • Create incident documentation templates • Conduct regular incident response training • Test incident response procedures regularly
5.25	**Assessment and decision on information security events**	Schools assess security incidents based on severity - a lost homework is minor, but leaked exam papers are critical. Clear guidelines help determine response levels, like how nurses assess student injuries from minor scrapes to serious accidents. **Information Security Connection:** Organizations need structured assessment processes for security events. Like schools categorizing incidents, companies must evaluate security events based on impact	• Create event assessment criteria and severity levels • Define decision-making authority for different severity levels • Establish response procedures for each severity level • Document assessment methods and decisions • Monitor patterns in security events • Review and update assessment criteria

		and urgency to determine appropriate response levels.	• regularly Train staff on incident assessment procedures • Maintain incident assessment records
5.26	**Response to information security incidents**	Schools have specific responses for different incidents - immediate action for cyberbullying posts, systematic response for compromised grade systems, and structured approach for lost confidential records. **Information Security Connection:** Organizations must have defined responses for security incidents. Like schools handling different security breaches, companies need clear procedures for containment, investigation, and recovery from security incidents.	• Develop incident response procedures • Define containment strategies • Establish investigation processes • Create recovery procedures • Set up communication protocols • Define escalation procedures • Document incident handling steps • Review and update response plans
5.27	**Learning from information security incident**	Schools analyse past incidents to improve - learning from a data breach to strengthen access controls or improving email security after a phishing incident. Like updating school safety rules after accidents, each incident becomes a learning opportunity. **Information Security Connection:** Organizations must use incidents to strengthen security. Like schools improving procedures after incidents, companies should analyse root causes, identify control weaknesses, and implement improvements based on lessons learned.	• Document detailed incident analysis • Identify root causes and patterns • Develop improvement recommendations • Update security controls based on lessons • Share lessons learned with relevant teams • Track implementation of improvements • Measure effectiveness of changes • Review incident trends periodically
5.28	**Collection of evidence**	Schools maintain proper evidence when investigating incidents - preserving CCTV footage of misconduct, keeping copies of inappropriate emails, documenting witness statements. Like maintaining chain of custody for lost property, evidence handling follows strict procedures. **Information Security Connection:** Organizations need proper evidence collection procedures.	• Establish evidence collection procedures • Define chain of custody process • Train staff on evidence handling • Set up secure evidence storage • Document evidence collection steps • Maintain evidence inventory

		Like schools documenting incidents, companies must preserve digital and physical evidence following forensic principles to support investigations and potential legal actions.	• Define evidence retention periods • Create evidence disposal procedures
5.29	**Information security during disruption**	Schools maintain security during disruptions like power outages or natural disasters. Even during emergencies, student records remain secure, exam materials protected, and confidential information safeguarded. **Information Security Connection:** Organizations must maintain security controls during disruptions. Like schools protecting information during emergencies, companies need plans to maintain security during crisis situations.	• Identify critical security controls • Create disruption response procedures • Establish minimum security requirements • Define emergency access procedures • Test security measures during disruptions • Document emergency procedures • Train staff on emergency protocols • Review and update plans regularly
5.30	**ICT readiness for business continuity**	Schools ensure critical systems stay operational - backup systems for student records, alternative methods for grade processing, and redundant communication systems. Like having backup generators for power failures, schools maintain educational continuity. **Information Security Connection:** Organizations must ensure ICT systems support business continuity. Like schools maintaining critical educational systems, companies need resilient ICT infrastructure to support operations during disruptions.	• Identify critical ICT services • Set recovery time objectives • Implement backup systems • Establish alternate processing sites • Create recovery procedures • Test continuity plans • Maintain backup equipment • Document recovery steps
5.31	**Legal, statutory, regulatory and contractual requirements**	Schools must comply with various requirements - education laws, student privacy regulations, health and safety rules. Like maintaining proper licenses for educational software, schools track and meet all legal obligations. **Information Security Connection:** Organizations must identify and comply with all relevant requirements. Like schools	• Identify applicable requirements • Document compliance obligations • Track regulatory changes • Implement compliance controls • Conduct regular compliance reviews • Maintain compliance records

		following education regulations, companies need to track and comply with security-related laws, regulations, and contractual obligations.	• Train staff on requirements • Update procedures as needed
5.32	**Intellectual property rights**	Schools respect and protect intellectual property - properly licensed textbooks, authorized use of educational materials, and protection of teachers' original content. Like managing library book copyrights, schools ensure proper use of all intellectual property. **Information Security Connection:** Organizations must protect intellectual property rights. Like schools managing educational material licenses, companies need to track software licenses, protect proprietary information, and ensure compliance with copyright laws.	• Document all intellectual property assets • Track software licenses and usage • Establish copyright compliance procedures • Monitor unauthorized software use • Train staff on IP rights • Maintain license inventory • Review compliance regularly • Handle violations appropriately
5.33	**Protection of records**	Schools protect various records - student files, staff records, financial documents, and administrative records. Each type has specific retention periods and protection requirements, like maintaining past student records for verification purposes. **Information Security Connection:** Organizations must protect records throughout their lifecycle. Like schools protecting student records, companies need to secure important records with appropriate retention periods and security controls.	• Identify critical records • Define retention periods • Implement protection controls • Establish storage procedures • Create access controls • Monitor record handling • Set disposal procedures Document record locations
5.34	**Privacy and protection of personal identifiable information (Pii)**	Schools handle sensitive personal information - student health records, family details, academic records. Like protecting student medical records, schools ensure personal information is accessed only by authorized staff and used appropriately. **Information Security Connection:** Organizations must protect	• Identify all PII handled • Create privacy protection policies • Implement data protection controls • Train staff on privacy requirements • Monitor PII handling • Respond to privacy requests

		personal information. Like schools safeguarding student data, companies need strong controls for collecting, using, and protecting personal information of employees and customers.	• Document PII processing • Regular privacy reviews
5.35	**Independent review of information security**	Schools undergo regular independent audits - education board reviews, safety inspections, and external security assessments. Like health and safety inspections, these reviews ensure security measures are working effectively. **Information Security Connection:** Organizations need independent security reviews. Like schools being audited for compliance, companies should have external parties review their security controls to ensure effectiveness.	• Schedule regular security reviews • Define review scope Select independent reviewers • Document review findings • Create improvement plans • Track implementation • Report results to management • Follow up on recommendations
5.36	**Compliance with policies, rules and standards for information security**	Schools ensure compliance with internal policies - from classroom rules to safety procedures. Regular checks confirm if teachers follow grading policies, staff follow security procedures, and everyone adheres to school rules. **Information Security Connection:** Organizations must ensure compliance with security policies. Like schools monitoring adherence to rules, companies need to verify that security policies are understood and followed.	• Regular compliance checks • Monitor policy adherence • Document compliance status • Address non-compliance • Update policies as needed • Train on policy changes • Maintain compliance records • Review effectiveness
5.37	**Documented operating procedures**	Schools maintain clear procedures for daily operations - from morning assembly to emergency evacuation. Step-by-step instructions ensure consistent operations, like having standard procedures for handling student records or conducting exams. **Information Security Connection:** Organizations need documented security procedures. Like schools having standard operating procedures, companies need clear,	• Document key procedures • Make procedures accessible • Train staff on procedures Update when changes occur • Review regularly • Maintain version control • Get management approval • Monitor procedure effectiveness

		written procedures for security-related operations to ensure consistency and reliability.	

DID YOU FIND THIS CHECKLIST USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

WWW.MINISTRYOFSECURITY.CO