Sample evidence pack

Latore LTD

This is a sample built from the fictional Latore LTD demo company, not a customer and not an audit opinion.

The pages that follow show the records an auditor opens in the workspace: the statement of applicability, an extract of the risk register, the key risk indicators, the management review, and the NIS2 Article 21 mapping.

Contents

1. Statement of applicability
2. Risk register extract
3. Key risk indicators
4. Management review
5. NIS2 Article 21 mapping

Each control in the statement of applicability has a decision on whether it applies, a status, and a written reason. The risk register extract, indicators, and management review sit beside those controls.

1. Statement of applicability

ISO 27001 Annex A for Latore LTD. Every control has a written justification.

93 controls.

Implemented: 36
In progress: 35
Not implemented: 18
Not applicable: 4

A.5.1 Policies for information security

Applicable · Implemented

Applies to the management system for the customer platform, the support desk, and the two offices. Publish the security rules leadership has approved, and make sure people can find them.

A.5.2 Information security roles and responsibilities

Applicable · In progress

Applies to the management system for the customer platform, the support desk, and the two offices. Name the people accountable for security work and tell them what they own.

A.5.3 Segregation of duties

Applicable · Implemented

Applies to the management system for the customer platform, the support desk, and the two offices. Split sensitive tasks so the same person cannot both request and approve them.

A.5.4 Management responsibilities

Applicable · Not implemented

Applies to the management system for the customer platform, the support desk, and the two offices. Managers make sure their own teams follow the security rules that apply to the work.

A.5.5 Contact with authorities

Applicable · In progress

Applies to the management system for the customer platform, the support desk, and the two offices. Keep an up-to-date list of regulators and law-enforcement contacts, and know when to use it.

A.5.6 Contact with special interest groups

Not applicable · Not applicable

The organisation does not belong to a specialist security forum. Supplier threat notices are reviewed under threat intelligence instead.

A.5.7 Threat intelligence

Applicable · Implemented

Applies to the management system for the customer platform, the support desk, and the two offices. Collect and review information about threats that could affect this organisation.

A.5.8 Information security in project management

Applicable · In progress

Applies to the management system for the customer platform, the support desk, and the two offices. Put security tasks into projects from the start, rather than after go-live.

A.5.9 Inventory of information and other associated assets

Applicable · Implemented

Applies to the management system for the customer platform, the support desk, and the two offices. Keep a list of the information the organisation depends on and the assets that hold it.

A.5.10 Acceptable use of information and other associated assets

Applicable · Not implemented

Applies to the management system for the customer platform, the support desk, and the two offices. Write down how people are allowed to use information and equipment.

A.5.11 Return of assets

Applicable · In progress

Applies to the management system for the customer platform, the support desk, and the two offices. Get equipment and access back when someone leaves or a contract ends.

A.5.12 Classification of information

Applicable · Implemented

Applies to the management system for the customer platform, the support desk, and the two offices. Mark information by how sensitive it is so people know how to handle it.

A.5.13 Labelling of information
Applicable · In progress
Applies to the management system for the customer platform, the support desk, and the two offices. Put the classification where people can see it on documents and data.

A.5.14 Information transfer
Applicable · Implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Protect information when it is sent inside the organisation or to someone outside.

A.5.15 Access control
Applicable · Not implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Decide who may reach which information, based on the work they do.

A.5.16 Identity management
Applicable · In progress
Applies to the management system for the customer platform, the support desk, and the two offices. Give each person a unique identity and close it when they no longer need it.

A.5.17 Authentication information
Applicable · Implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Look after passwords and other secrets so they stay hard to guess or steal.

A.5.18 Access rights
Applicable · In progress
Applies to the management system for the customer platform, the support desk, and the two offices. Grant, review, and remove access so people keep only what the role needs.

A.5.19 Information security in supplier relationships
Applicable · Implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Set security expectations for suppliers and check that they are being met.

A.5.20 Addressing information security within supplier agreements
Applicable · Not implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Write the supplier's security duties into the contract, including what happens if they are missed.

A.5.21 Managing information security in the ICT supply chain
Applicable · In progress
Applies to the management system for the customer platform, the support desk, and the two offices. Understand security risks that arrive through the chain of technology suppliers.

A.5.22 Monitoring, review and change management of supplier services
Applicable · Implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Review supplier services on a schedule and control the changes they make.

A.5.23 Information security for use of cloud services
Applicable · In progress
Applies to the management system for the customer platform, the support desk, and the two offices. Decide how cloud services are chosen, used, and left, including where the data sits.

A.5.24 Information security incident management planning and preparation
Applicable · Implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Agree roles, steps, and contacts before an incident happens.

A.5.25 Assessment and decision on information security events
Applicable · Not implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Decide whether an event is an incident and choose the next step.

A.5.26 Response to information security incidents
Applicable · In progress
Applies to the management system for the customer platform, the support desk, and the two offices. Follow the prepared steps to contain an incident and restore the service.

A.5.27 Learning from information security incidents
Applicable · Implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Record what happened and change the way of working so it is less likely again.

A.5.28 Collection of evidence
Applicable · In progress
Applies to the management system for the customer platform, the support desk, and the two offices. Gather and keep evidence from an incident so it can be used later.

A.5.29 Information security during disruption
Applicable · Implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Keep security in place while the organisation is running in a fallback mode.

A.5.30 ICT readiness for business continuity
Applicable · Not implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Plan and test that technology can be recovered in line with what the business needs.

A.5.31 Legal, statutory, regulatory and contractual requirements
Applicable · In progress
Applies to the management system for the customer platform, the support desk, and the two offices. Know the legal and contractual security duties that apply, and meet them.

A.5.32 Intellectual property rights
Applicable · Implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Use software and other material only where the organisation actually has the rights.

A.5.33 Protection of records
Applicable · In progress
Applies to the management system for the customer platform, the support desk, and the two offices. Keep records safe and retrievable for as long as the business or the law needs them.

A.5.34 Privacy and protection of PII
Applicable · Implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Handle personal data in line with the privacy duties that apply to it.

A.5.35 Independent review of information security
Applicable · Not implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Have someone independent look at the security arrangements on a planned cycle.

A.5.36 Compliance with policies, rules and standards for information security
Applicable · In progress
Applies to the management system for the customer platform, the support desk, and the two offices. Check that people and systems follow the organisation's own security rules.

A.5.37 Documented operating procedures
Applicable · Implemented
Applies to the management system for the customer platform, the support desk, and the two offices. Write down how to run the systems so the work can be repeated the same way.

A.6.1 Screening
Applicable · In progress
Applies to employees and contractors who can reach customer or platform information. Check candidates and contractors to a depth that matches the access they will have.

A.6.2 Terms and conditions of employment
Applicable · Implemented
Applies to employees and contractors who can reach customer or platform information. Put security duties into employment or contractor terms before the work starts.

A.6.3 Information security awareness, education and training
Applicable · Not implemented
Applies to employees and contractors who can reach customer or platform information. Train people so they recognise the threats and know what they are expected to do.

A.6.4 Disciplinary process
Applicable · In progress
Applies to employees and contractors who can reach customer or platform information. Have a fair process for someone who breaks the security rules.

A.6.5 Responsibilities after termination or change of employment
Applicable · Implemented
Applies to employees and contractors who can reach customer or platform information. When a role ends or changes, remove access and remind the person of duties that still apply.

A.6.6 Confidentiality or non-disclosure agreements
Applicable · In progress
Applies to employees and contractors who can reach customer or platform information. Use a written confidentiality term for anyone who will see sensitive information.

A.6.7 Remote working
Applicable · Implemented
Applies to employees and contractors who can reach customer or platform information. Set rules so work done away from the office stays protected.

A.6.8 Information security event reporting
Applicable · Not implemented
Applies to employees and contractors who can reach customer or platform information. Make it easy, and expected, for people to report security events quickly.

A.7.1 Physical security perimeters
Applicable · In progress
Applies to the two offices and the equipment kept there. Define the boundary of each secure area and control how people cross it.

A.7.2 Physical entry
Applicable · Implemented
Applies to the two offices and the equipment kept there. Let people into secure areas only when they are allowed to be there.

A.7.3 Securing offices, rooms and facilities
Applicable · In progress
Applies to the two offices and the equipment kept there. Lock the rooms and facilities that hold sensitive work or equipment.

A.7.4 Physical security monitoring
Applicable · Implemented
Applies to the two offices and the equipment kept there. Watch physical areas so an unauthorised entry can be noticed.

A.7.5 Protecting against physical and environmental threats
Applicable · Not implemented
Applies to the two offices and the equipment kept there. Protect sites against fire, flood, and similar physical threats.

A.7.6 Working in secure areas
Not applicable · Not applicable
No room is designated as a secure area. The offices use badge entry and a clear-desk rule, which are recorded on their own controls.

A.7.7 Clear desk and clear screen
Applicable · In progress
Applies to the two offices and the equipment kept there. Put papers away and lock screens so a passer-by cannot read them.

A.7.8 Equipment siting and protection
Applicable · Implemented
Applies to the two offices and the equipment kept there. Place equipment where it is harder to damage, steal, or overlook.

A.7.9 Security of assets off-premises
Applicable · In progress
Applies to the two offices and the equipment kept there. Protect equipment and information that leave the site.

A.7.10 Storage media
Applicable · Implemented
Applies to the two offices and the equipment kept there. Store, move, and dispose of disks and other media without exposing what is on them.

A.7.11 Supporting utilities
Applicable · Not implemented
Applies to the two offices and the equipment kept there. Keep power, cooling, and the other utilities reliable enough for the systems that need them.

A.7.12 Cabling security
Applicable · In progress
Applies to the two offices and the equipment kept there. Protect power and network cables from damage and from tapping.

A.7.13 Equipment maintenance
Applicable · Implemented
Applies to the two offices and the equipment kept there. Maintain equipment so it keeps working, and stays secure, while it is being serviced.

A.7.14 Secure disposal or re-use of equipment
Applicable · In progress
Applies to the two offices and the equipment kept there. Wipe or destroy storage before equipment is reused or thrown away.

A.8.1 User endpoint devices
Applicable · Implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Set the rules for laptops, phones, and other devices people use for work.

A.8.2 Privileged access rights
Applicable · Not implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Limit administrator rights and review who still has them.

A.8.3 Information access restriction
Applicable · In progress
Applies to the hosted platform, the support tools, and the devices used to run them. Limit access to information and to system functions to the people who need them.

A.8.4 Access to source code
Applicable · Implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Limit who can read or change source code.

A.8.5 Secure authentication
Applicable · In progress
Applies to the hosted platform, the support tools, and the devices used to run them. Use sign-in methods that match the risk, including a second factor where it matters.

A.8.6 Capacity management
Applicable · Implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Watch capacity so systems keep up with the demand placed on them.

A.8.7 Protection against malware
Applicable · Not implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Protect systems against malware and keep that protection current.

A.8.8 Management of technical vulnerabilities
Applicable · In progress
Applies to the hosted platform, the support tools, and the devices used to run them. Find technical weaknesses and deal with the ones that matter.

A.8.9 Configuration management
Applicable · Implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Set a secure configuration and control later changes to it.

A.8.10 Information deletion
Applicable · In progress
Applies to the hosted platform, the support tools, and the devices used to run them. Delete information when it is no longer needed so copies do not linger.

A.8.11 Data masking
Not applicable · Not applicable
Production data is not copied into an environment where masking would be the control. Access to the live data is limited instead.

A.8.12 Data leakage prevention
Applicable · Implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Reduce the chance that sensitive information leaves by mistake.

A.8.13 Information backup
Applicable · Not implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Take backups and test that they can actually be restored.

A.8.14 Redundancy of information processing facilities
Applicable · In progress
Applies to the hosted platform, the support tools, and the devices used to run them. Provide spare capacity for the systems the business cannot pause.

A.8.15 Logging
Applicable · Implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Record the events that help detect and investigate a security problem.

A.8.16 Monitoring activities
Applicable · In progress
Applies to the hosted platform, the support tools, and the devices used to run them. Watch networks and systems for unusual activity and act on it.

A.8.17 Clock synchronization
Applicable · Implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Keep system clocks aligned so logs and evidence agree on the time.

A.8.18 Use of privileged utility programs
Applicable · Not implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Restrict tools that can bypass the normal security controls.

A.8.19 Installation of software on operational systems
Applicable · In progress
Applies to the hosted platform, the support tools, and the devices used to run them. Control which software can be installed on live systems.

A.8.20 Networks security
Applicable · Implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Protect the network and separate traffic that does not belong together.

A.8.21 Security of network services
Applicable · In progress
Applies to the hosted platform, the support tools, and the devices used to run them. Agree the security features with whoever provides the network services.

A.8.22 Segregation of networks
Applicable · Implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Separate groups of systems that have different security needs.

A.8.23 Web filtering
Not applicable · Not applicable
There is no separate web filter. Browsing risk on managed devices is handled with endpoint protection.

A.8.24 Use of cryptography
Applicable · Not implemented
Applies to the hosted platform, the support tools, and the devices used to run them. Define how encryption is used to protect information.

A.8.25 Secure development life cycle
Applicable · In progress
Applies to the hosted platform, the support tools, and the devices used to run them. Build security checks into the way software is developed.

A.8.26 Application security requirements

Applicable · Implemented

Applies to the hosted platform, the support tools, and the devices used to run them. State the security needs when an application is built or bought.

A.8.27 Secure system architecture and engineering principles

Applicable · In progress

Applies to the hosted platform, the support tools, and the devices used to run them. Apply the agreed design principles when systems are engineered.

A.8.28 Secure coding

Applicable · Implemented

Applies to the hosted platform, the support tools, and the devices used to run them. Follow coding rules that avoid the common security mistakes.

A.8.29 Security testing in development and acceptance

Applicable · Not implemented

Applies to the hosted platform, the support tools, and the devices used to run them. Test security before a system is accepted into use.

A.8.30 Outsourced development

Applicable · In progress

Applies to the hosted platform, the support tools, and the devices used to run them. Supervise development work that another organisation does.

A.8.31 Separation of development, test and production environments

Applicable · Implemented

Applies to the hosted platform, the support tools, and the devices used to run them. Keep development, test, and live environments apart.

A.8.32 Change management

Applicable · In progress

Applies to the hosted platform, the support tools, and the devices used to run them. Approve and record changes to systems before they reach the live service.

A.8.33 Test information

Applicable · Implemented

Applies to the hosted platform, the support tools, and the devices used to run them. Protect any real data used in testing, or use data that is not real.

A.8.34 Protection of information systems during audit testing

Applicable · Not implemented

Applies to the hosted platform, the support tools, and the devices used to run them. Plan audit tests so they do not knock over live systems.

2. Risk register extract

Three risks recorded for the HR platform, with the treatment chosen and the residual score after that treatment. Likelihood and impact are each scored from 1 to 5. The score is their product.

Example HR platform: staff directory leak enables targeted phishing

Reference DEMO-RA-HR-001

A leaked staff directory from the HR platform lets an attacker impersonate HR, IT, or a manager.

Treatment: Accept. Status: Approved. Inherent score 12 (High). Residual score 4 (Low).

Example HR platform: candidate data kept longer than needed

Reference DEMO-RA-HR-002

The supplier retains candidate CVs and contact details for years after the role is filled.

Treatment: Mitigate. Status: Reviewed. Inherent score 9 (Medium). Residual score 4 (Low).

Example HR platform: supplier staff access not revoked

Reference DEMO-RA-HR-003

Named supplier support staff keep access to employee records after they leave the supplier.

Treatment: Mitigate. Status: Reviewed. Inherent score 8 (Medium). Residual score 3 (Low).

Treatment notes

DEMO-RA-002. Effectiveness: the callback check stopped the test payment change. The control is in place.

DEMO-RA-009. Effectiveness: the sampled laptops reported disk encryption on the last review.

DEMO-RA-016. Effectiveness: the last restore drill brought the sample mailbox back inside the agreed window.

Assets named on the register

Customer support team
People. Owner: Head of Support. Criticality: High. Support desk that can see customer accounts. Counted as a people asset.

Example card processor
Supplier. Owner: Procurement Lead. Criticality: High. Payments processor used for customer billing.

Example hosting provider
Supplier. Owner: Head of Platform. Criticality: High. Hosting provider for the customer platform.

3. Key risk indicators

The current reading against the threshold the workspace agreed.

Critical patches overdue · Amber

Critical patches still open after the agreed window.
Current reading: 1. Owner: IT Operations Lead.
Green: 0. Amber: 1–3. Red: more than 3.

Phishing exercise result · Amber

Latest exercise compared with the limit set in the awareness plan.
Current reading: at the agreed limit. Owner: CISO.
Green: below the agreed limit. Amber: at the agreed limit. Red: above the agreed limit.

Backup restore test · Green

Whether the latest restore drill met the agreed window.
Current reading: last drill succeeded. Owner: Head of Infrastructure.
Green: last drill succeeded. Amber: drill due this quarter. Red: drill missed or restore failed.

Open high risks past review · Amber

High or critical risks whose review date has passed.
Current reading: 2. Owner: CISO.
Green: 0. Amber: 1–2. Red: more than 2.

4. Management review

ISMS management review

MR-2026-001. Held on 2026-09-16. Next review 2027-03-16. Status: Completed.

Attendees: CISO, Head of Platform, DPO, IT Operations Lead.

Inputs

- Actions from the previous review are closed, or they are still on the treatment plan.
- The scope is unchanged: customer platform, hosting, support desk, and the two offices.
- Customer questions this quarter were about backup restore and supplier access.
- Risks above the medium band are on the treatment plan, each with an owner.
- The support desk asked for a clearer leaver checklist.
- Opportunity: run the restore drill on a second system before the next review.

Decisions

- Keep the window for critical patches at 14 days.
- The procurement lead may accept the recorded supplier residual, and will review it within six months.
- Hold the next management review on 16 March 2027.
- The infrastructure lead will run the next restore drill before that review.

5. NIS2 Article 21 mapping

The Article 21 security measures named for this sample, and the short description recorded against each one.

NIS2-ART21-1 Risk Analysis and Information System Security Policies
Article 21(2)(a)
Policies on risk analysis and information system security shall be established, documented, and reviewed regularly.

NIS2-ART21-2 Incident Handling and Emergency Escalation
Article 21(2)(b)
Incident handling processes for prevention, detection, and response to security incidents shall be established.

NIS2-ART21-3 Business Continuity and Crisis Management
Article 21(2)(c)
Business continuity processes such as backup management, disaster recovery, and crisis management shall be maintained.

NIS2-ART21-4 Supply Chain Security and Vendor Due Diligence
Article 21(2)(d)
Supply chain security including security-related aspects concerning relationships with direct suppliers and service providers.

NIS2-ART21-5 Security in Network and Information Systems Acquisition
Article 21(2)(e)
Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.

NIS2-ART21-6 Cybersecurity Risk Management Effectiveness Testing
Article 21(2)(f)
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.

NIS2-ART21-7 Cyber Hygiene and Training
Article 21(2)(g)
Basic cyber hygiene practices and cybersecurity training across the organization.

NIS2-ART21-8 Use of Cryptography and Encryption
Article 21(2)(h)
Policies and procedures regarding the use of cryptography and, where appropriate, encryption.

NIS2-ART21-9 Human Resources Security and Access Control
Article 21(2)(i)
Human resources security, access control policies and asset management.

NIS2-ART21-10 Multi-Factor Authentication and Secured Communications
Article 21(2)(j)
The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications.