GapLedger

Statement of Applicability

Example Analytics Ltd (fictional sample): Organization-wide ISMS

Frameworks in scope: ISO
Generated 2026-09-24 17:41 UTC by GapLedger (sample data, fictional company)

Applicability decisions and justifications are the organization's responsibility. Point-in-time snapshot.

101 of 111 controls applicable · 2 applicable but treating no recorded risk

ISMS Management (Cl. 4-10)

[Applicable] CL.4.1 Know your context — including climate — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.4.3 Define your ISMS scope — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.5.1 Leadership owns it — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.5.2 Publish a security policy — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.5.3 Assign roles and authority — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.6.1.2 Assess your risks — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.6.1.3 Treat risks and state applicability — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.6.2 Set security objectives — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.6.3 Plan changes — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.7.2 Make sure people are competent — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.7.3 Keep people aware — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.7.4 Communicate — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.7.5 Control your documents — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.9.1 Measure performance — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.9.2 Audit yourself — In progress
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.9.3 Review at the top — In progress
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.10.1 Keep improving — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

[Applicable] CL.10.2 Fix and prevent — Implemented
Justification: Applicable: mandatory ISO 27001 management-system requirement.

Organizational

[Applicable] A.5.1 Set your security policy — Implemented
Justification: Applicable: selected to treat R-14.
Treats: R-14 Staff unaware of their security obligations

[Applicable] A.5.2 Name who's responsible — Implemented
Justification: Applicable: selected to treat R-14.
Treats: R-14 Staff unaware of their security obligations

[Applicable] A.5.3 Separate conflicting duties — Implemented
Justification: Applicable: selected to treat R-12.
Treats: R-12 Unauthorised or unreviewed change to production

[Applicable] A.5.4 Hold people to the policy — Implemented
Justification: Applicable: selected to treat R-14.
Treats: R-14 Staff unaware of their security obligations

[Applicable] A.5.5 Keep authority contacts — Implemented
Justification: Applicable: selected to treat R-15.
Treats: R-15 Changes in threats or obligations go unnoticed

[Applicable] A.5.6 Stay plugged in — Implemented
Justification: Applicable: selected to treat R-15.
Treats: R-15 Changes in threats or obligations go unnoticed

[Applicable] A.5.7 Watch the threats — In progress
Justification: Applicable: selected to treat R-15.
Treats: R-15 Changes in threats or obligations go unnoticed

[Applicable] A.5.8 Build security into projects — Implemented
Justification: Applicable: selected to treat R-13.
Treats: R-13 Security requirements missed in new features

[Applicable] A.5.9 Inventory your assets — Implemented
Justification: Applicable: selected to treat R-02, R-05.
Treats: R-02 Customer data exposed by a misconfigured cloud resource; R-05 Lost or stolen laptop holding customer data

[Applicable] A.5.10 Set acceptable-use rules — Implemented
Justification: Applicable: selected to treat R-05, R-14.
Treats: R-05 Lost or stolen laptop holding customer data; R-14 Staff unaware of their security obligations

[Applicable] A.5.11 Get assets back — Implemented
Justification: Applicable: selected to treat R-06.
Treats: R-06 Former employee keeps access after leaving

[Applicable] A.5.12 Classify information — Implemented
Justification: Applicable: selected to treat R-11.
Treats: R-11 Sensitive information shared through the wrong channel

[Applicable] A.5.13 Label information — Implemented
Justification: Applicable: selected to treat R-11.
Treats: R-11 Sensitive information shared through the wrong channel

[Applicable] A.5.14 Transfer information safely — Implemented
Justification: Applicable: selected to treat R-11.
Treats: R-11 Sensitive information shared through the wrong channel

[Applicable] A.5.15 Control access — Implemented
Justification: Applicable: selected to treat R-01.
Treats: R-01 Phishing leads to a compromised staff account

[Applicable] A.5.16 Manage identities — Implemented
Justification: Applicable: selected to treat R-06.
Treats: R-06 Former employee keeps access after leaving

[Applicable] A.5.17 Protect credentials — Implemented
Justification: Applicable: selected to treat R-01.
Treats: R-01 Phishing leads to a compromised staff account

[Applicable] A.5.18 Grant least privilege — Implemented
Justification: Applicable: selected to treat R-06.
Treats: R-06 Former employee keeps access after leaving

[Applicable] A.5.19 Vet your suppliers — Implemented
Justification: Applicable: selected to treat R-07.
Treats: R-07 A key supplier (hosting, email, payments) suffers a breach

[Applicable] A.5.20 Put it in supplier contracts — Implemented
Justification: Applicable: selected to treat R-07.
Treats: R-07 A key supplier (hosting, email, payments) suffers a breach

[Applicable] A.5.21 Secure the ICT supply chain — In progress
Justification: Applicable: selected to treat R-07.
Treats: R-07 A key supplier (hosting, email, payments) suffers a breach

[Applicable] A.5.22 Watch your suppliers — Implemented
Justification: Applicable: selected to treat R-07.
Treats: R-07 A key supplier (hosting, email, payments) suffers a breach

[Applicable] A.5.23 Secure your cloud use — Implemented
Justification: Applicable: selected to treat R-02, R-07.
Treats: R-02 Customer data exposed by a misconfigured cloud resource; R-07 A key supplier (hosting, email, payments) suffers a breach

[Applicable] A.5.24 Plan for incidents — Implemented
Justification: Applicable: selected to treat R-08.
Treats: R-08 Security incident detected late or handled poorly

[Applicable] A.5.25 Triage events — Implemented
Justification: Applicable: selected to treat R-08.
Treats: R-08 Security incident detected late or handled poorly

[Applicable] A.5.26 Respond to incidents — Implemented
Justification: Applicable: selected to treat R-08.
Treats: R-08 Security incident detected late or handled poorly

[Applicable] A.5.27 Learn from incidents — Implemented
Justification: Applicable: selected to treat R-08.
Treats: R-08 Security incident detected late or handled poorly

[Applicable] A.5.28 Preserve evidence — Implemented

Justification: Applicable: selected to treat R-08.
Treats: R-08 Security incident detected late or handled poorly

[Applicable] A.5.29 Stay secure in a crisis — Implemented
Justification: Applicable: selected to treat R-10.
Treats: R-10 Production outage beyond customer service levels

[Applicable] A.5.30 Be ready to recover IT — Implemented
Justification: Applicable: selected to treat R-03, R-10.
Treats: R-03 Ransomware or destructive attack on production; R-10 Production outage beyond customer service levels

[Applicable] A.5.31 Know your obligations — Implemented
Justification: Applicable: selected to treat R-09.
Treats: R-09 Personal data processed in breach of privacy law

[Applicable] A.5.32 Respect IP — Implemented
Justification: Applicable: expected practice for a SaaS provider handling customer data.
Treats: — no risk recorded —

[Applicable] A.5.33 Protect records — Implemented
Justification: Applicable: selected to treat R-09.
Treats: R-09 Personal data processed in breach of privacy law

[Applicable] A.5.34 Protect personal data — Implemented
Justification: Applicable: selected to treat R-09.
Treats: R-09 Personal data processed in breach of privacy law

[Applicable] A.5.35 Get an independent check — Not started
Justification: Applicable: selected to treat R-15.
Treats: R-15 Changes in threats or obligations go unnoticed

[Applicable] A.5.36 Check compliance — In progress
Justification: Applicable: selected to treat R-15.
Treats: R-15 Changes in threats or obligations go unnoticed

[Applicable] A.5.37 Write down procedures — Implemented
Justification: Applicable: selected to treat R-14.
Treats: R-14 Staff unaware of their security obligations

People

[Applicable] A.6.1 Screen on hire — Implemented
Justification: Applicable: selected to treat R-14.
Treats: R-14 Staff unaware of their security obligations

[Applicable] A.6.2 Put it in the contract — Implemented
Justification: Applicable: selected to treat R-14.
Treats: R-14 Staff unaware of their security obligations

[Applicable] A.6.3 Train your people — Implemented
Justification: Applicable: selected to treat R-01.
Treats: R-01 Phishing leads to a compromised staff account

[Applicable] A.6.4 Have a disciplinary process — Implemented
Justification: Applicable: selected to treat R-14.
Treats: R-14 Staff unaware of their security obligations

[Applicable] A.6.5 Cover the exit — Implemented
Justification: Applicable: selected to treat R-06.
Treats: R-06 Former employee keeps access after leaving

[Applicable] A.6.6 Use NDAs — Implemented
Justification: Applicable: selected to treat R-11.
Treats: R-11 Sensitive information shared through the wrong channel

[Applicable] A.6.7 Secure remote work — Implemented
Justification: Applicable: selected to treat R-05.
Treats: R-05 Lost or stolen laptop holding customer data

[Applicable] A.6.8 Make it easy to report — Implemented
Justification: Applicable: selected to treat R-08.
Treats: R-08 Security incident detected late or handled poorly

Physical

[Excluded] A.7.1 Define secure perimeters — N/A
Justification: Excluded: the company operates no premises, server rooms or network cabling of its own. Production runs on a public cloud provider (see A.5.23) and staff work remotely or from a managed coworking space whose physical security is the landlord's responsibility under the lease.

[Excluded] A.7.2 Control who gets in — N/A
Justification: Excluded: the company operates no premises, server rooms or network cabling of its own. Production runs on a public cloud provider (see A.5.23) and staff work remotely or from a managed coworking space whose physical security is the landlord's responsibility under the lease.

[Excluded] A.7.3 Secure the spaces — N/A
Justification: Excluded: the company operates no premises, server rooms or network cabling of its own. Production runs on a public cloud provider (see A.5.23) and staff work remotely or from a managed coworking space whose physical security is the landlord's responsibility under the lease.

[Excluded] A.7.4 Monitor the premises — N/A
Justification: Excluded: the company operates no premises, server rooms or network cabling of its own. Production runs on a public cloud provider (see A.5.23) and staff work remotely or from a managed coworking space whose physical security is the landlord's responsibility under the lease.

[Excluded] A.7.5 Guard against the environment — N/A
Justification: Excluded: the company operates no premises, server rooms or network cabling of its own. Production runs on a public cloud provider (see A.5.23) and staff work remotely or from a managed coworking space whose physical security is the landlord's responsibility under the lease.

[Excluded] A.7.6 Set rules for secure areas — N/A
Justification: Excluded: the company operates no premises, server rooms or network cabling of its own. Production runs on a public cloud provider (see A.5.23) and staff work remotely or from a managed coworking space whose physical security is the landlord's responsibility under the lease.

[Applicable] A.7.7 Clear desks and screens — Implemented
Justification: Applicable: selected to treat R-05.
Treats: R-05 Lost or stolen laptop holding customer data

[Excluded] A.7.8 Site equipment safely — N/A
Justification: Excluded: the company operates no premises, server rooms or network cabling of its own. Production runs on a public cloud provider (see A.5.23) and staff work remotely or from a managed coworking space whose physical security is the landlord's responsibility under the lease.

[Applicable] A.7.9 Protect assets off-site — Implemented
Justification: Applicable: selected to treat R-05.
Treats: R-05 Lost or stolen laptop holding customer data

[Applicable] A.7.10 Manage storage media — Implemented
Justification: Applicable: selected to treat R-05.
Treats: R-05 Lost or stolen laptop holding customer data

[Excluded] A.7.11 Protect your utilities — N/A
Justification: Excluded: the company operates no premises, server rooms or network cabling of its own. Production runs on a public cloud provider (see A.5.23) and staff work remotely or from a managed coworking space whose physical security is the landlord's responsibility under the lease.

[Excluded] A.7.12 Protect cabling — N/A
Justification: Excluded: the company operates no premises, server rooms or network cabling of its own. Production runs on a public cloud provider (see A.5.23) and staff work remotely or from a managed coworking space whose physical security is the landlord's responsibility under the lease.

[Applicable] A.7.13 Maintain equipment — Implemented
Justification: Applicable: expected practice for a SaaS provider handling customer data.
Treats: — no risk recorded —

[Applicable] A.7.14 Wipe before disposal — Implemented
Justification: Applicable: selected to treat R-05.
Treats: R-05 Lost or stolen laptop holding customer data

Technological

[Applicable] A.8.1 Secure endpoints — Implemented
Justification: Applicable: selected to treat R-05.
Treats: R-05 Lost or stolen laptop holding customer data

[Applicable] A.8.2 Limit admin rights — Implemented
Justification: Applicable: selected to treat R-06, R-12.
Treats: R-06 Former employee keeps access after leaving; R-12 Unauthorised or unreviewed change to production

[Applicable] A.8.3 Restrict access to data — Implemented
Justification: Applicable: selected to treat R-02.
Treats: R-02 Customer data exposed by a misconfigured cloud resource

[Applicable] A.8.4 Guard source code — Implemented
Justification: Applicable: selected to treat R-12.
Treats: R-12 Unauthorised or unreviewed change to production

[Applicable] A.8.5 Authenticate securely — Implemented
Justification: Applicable: selected to treat R-01.
Treats: R-01 Phishing leads to a compromised staff account

[Applicable] A.8.6 Manage capacity — Implemented
Justification: Applicable: selected to treat R-10.
Treats: R-10 Production outage beyond customer service levels

[Applicable] A.8.7 Block malware — Implemented
Justification: Applicable: selected to treat R-01, R-03.
Treats: R-01 Phishing leads to a compromised staff account; R-03 Ransomware or destructive attack on production

[Applicable] A.8.8 Patch vulnerabilities — Implemented
Justification: Applicable: selected to treat R-03, R-04.
Treats: R-03 Ransomware or destructive attack on production; R-04 Vulnerable dependency exploited in the product

[Applicable] A.8.9 Harden configurations — Implemented
Justification: Applicable: selected to treat R-02.
Treats: R-02 Customer data exposed by a misconfigured cloud resource

[Applicable] A.8.10 Delete when done — Implemented

Justification: Applicable: selected to treat R-09.
Treats: R-09 Personal data processed in breach of privacy law

[Applicable] A.8.11 Mask sensitive data — In progress
Justification: Applicable: selected to treat R-09.
Treats: R-09 Personal data processed in breach of privacy law

[Applicable] A.8.12 Prevent data leaks — Implemented
Justification: Applicable: selected to treat R-02, R-11.
Treats: R-02 Customer data exposed by a misconfigured cloud resource; R-11 Sensitive information shared through the wrong channel

[Applicable] A.8.13 Back up and test restores — Implemented
Justification: Applicable: selected to treat R-03, R-10.
Treats: R-03 Ransomware or destructive attack on production; R-10 Production outage beyond customer service levels

[Applicable] A.8.14 Build in redundancy — Implemented
Justification: Applicable: selected to treat R-03, R-10.
Treats: R-03 Ransomware or destructive attack on production; R-10 Production outage beyond customer service levels

[Applicable] A.8.15 Keep logs — Implemented
Justification: Applicable: selected to treat R-08.
Treats: R-08 Security incident detected late or handled poorly

[Applicable] A.8.16 Monitor for anomalies — In progress
Justification: Applicable: selected to treat R-08.
Treats: R-08 Security incident detected late or handled poorly

[Applicable] A.8.17 Sync the clocks — Implemented
Justification: Applicable: selected to treat R-08.
Treats: R-08 Security incident detected late or handled poorly

[Applicable] A.8.18 Control power tools — Implemented
Justification: Applicable: selected to treat R-12.
Treats: R-12 Unauthorised or unreviewed change to production

[Applicable] A.8.19 Control software installs — Implemented
Justification: Applicable: selected to treat R-12.
Treats: R-12 Unauthorised or unreviewed change to production

[Applicable] A.8.20 Secure your networks — Implemented
Justification: Applicable: selected to treat R-02.
Treats: R-02 Customer data exposed by a misconfigured cloud resource

[Applicable] A.8.21 Secure network services — Implemented
Justification: Applicable: selected to treat R-02.
Treats: R-02 Customer data exposed by a misconfigured cloud resource

[Applicable] A.8.22 Segment networks — Implemented
Justification: Applicable: selected to treat R-02.
Treats: R-02 Customer data exposed by a misconfigured cloud resource

[Applicable] A.8.23 Filter web access — Implemented
Justification: Applicable: selected to treat R-01.
Treats: R-01 Phishing leads to a compromised staff account

[Applicable] A.8.24 Use encryption well — Implemented
Justification: Applicable: selected to treat R-02, R-05.
Treats: R-02 Customer data exposed by a misconfigured cloud resource; R-05 Lost or stolen laptop holding customer data

[Applicable] A.8.25 Develop securely — Implemented
Justification: Applicable: selected to treat R-04.
Treats: R-04 Vulnerable dependency exploited in the product

[Applicable] A.8.26 Define app security needs — Implemented
Justification: Applicable: selected to treat R-13.
Treats: R-13 Security requirements missed in new features

[Applicable] A.8.27 Engineer securely — Implemented
Justification: Applicable: selected to treat R-13.
Treats: R-13 Security requirements missed in new features

[Applicable] A.8.28 Code securely — Implemented
Justification: Applicable: selected to treat R-04.
Treats: R-04 Vulnerable dependency exploited in the product

[Applicable] A.8.29 Test security before go-live — Implemented
Justification: Applicable: selected to treat R-04.
Treats: R-04 Vulnerable dependency exploited in the product

[Excluded] A.8.30 Oversee outsourced dev — N/A
Justification: Excluded: no development is outsourced. All product code is written and reviewed by employees; contractors, if engaged, work under A.6.2 and the same controls as staff.

[Applicable] A.8.31 Separate environments — Implemented
Justification: Applicable: selected to treat R-13.
Treats: R-13 Security requirements missed in new features

[Applicable] A.8.32 Manage changes — Implemented
Justification: Applicable: selected to treat R-04, R-12.
Treats: R-04 Vulnerable dependency exploited in the product; R-12 Unauthorised or unreviewed change to production

[Applicable] A.8.33 Protect test data — In progress

Justification: Applicable: selected to treat R-13.

Treats: R-13 Security requirements missed in new features

[Applicable] A.8.34 Protect systems during audits — Not started

Justification: Applicable: selected to treat R-13.

Treats: R-13 Security requirements missed in new features

Compliance management software. Not legal advice, and not a certification body. Certification decisions rest with your accredited auditor; regulatory readiness is your organization's responsibility.