ISO

Noureddine Kanzari

ISO/IEC 27002:2022

Master the Essentials of Information Security Controls

Your Path to Achieving ISO/IEC 27001 Certification

Learn How to Avoid Minor and Major Non-Conformities

Part 2

Learn by Doing: Practical Guide

About the author

Noureddine Kanzari is a cybersecurity expert with an extensive background in IT risk management and cybersecurity instruction. With a diverse range of certifications that includes being a PECB Certified Trainer, DORA Senior Lead Manager, NIST Cybersecurity Consultant, Senior Lead Incident Manager, Senior Lead SOC 2 Analyst, Data Protection Officer (DPO), DORA Senior Lead Manager, ISO 42001 Senior Lead Auditor, ISO 42001 Senior Lead Implementer, Senior Lead SCADA Security Manager, ISO 22301 Senior Lead Implementer, ISO 22301 Senior Lead Auditor,EBIOS Risk Manager, ISO 27005 Senior Lead Risk Manager, ISO 27001 Senior Lead Implementer, ISO 27001 Senior Lead Auditor, Cisco Certified Specialist in Security Core and Enterprise Core, NSE4 Network Security Professional, Palo Alto Instructor, Devops Tools Engineer, LPIC-3 Enterprise Professional Security, LPIC-3 Enterprise Professional Virtualization & High Availability, LPIC-2, LPIC-1, Suse Certified Linux Administration, and a Certified Security Auditor in computer security,

Noureddine Kanzari's professional journey is characterized by a series of impactful roles and accomplishments. Throughout his career, he has held various pivotal positions, including:

Chief Information Security Officer (CISO)

Audit Team Leader

Cybersecurity Instructor

Technical Manager

Training Manager

His extensive experience and leadership have contributed significantly to enhancing cybersecurity practices, risk management strategies, and organizational resilience.

Contents

1. ORGANIZATIONAL CONTROLS

1.1 Management responsibilities (5.4)

Control 5.4:

Management shall require all personnel to implement information security measures in accordance with the organization's information security policy, specific policies and established procedures.

Control attributes:

- Control type: When it acts : Preventive
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Identify
- Optional capabilities: Which operational area it belongs to : Governance
- Security domains: Which domain it relates to : Governance andt Ecosystem

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventive	Confidentiality Integrity Availability	Identify	Gouvernance	Gouvernance and Ecosystem

Control description:

Top management must actively support information security to make it successful. Their visible leadership is critical, without it, information security efforts will eventually fail.

➔ Management must show that they truly support information security (not just talk about it). They need to make sure all employees understand and follow the organization's security rules.

➔ Management must ensure these things happen:

° Before someone gets access to company information, they must be trained about their security responsibilities.

° Employees must get clear instructions about what is expected from them regarding information security.

° Employees must be required to follow the organization's security policies.

° Employees must have enough awareness and knowledge about security, depending on their job role.

° Employees must follow the terms of their employment contracts, including all information security rules.

° Employees must keep improving their security skills through ongoing training

° There should be a confidential way for employees to report security problems or violations, even anonymously if needed.

° Employees should be given enough time, tools, and support to properly implement security controls.

Control evidence:

Checks to be performed	Evidence
➢ If management explicitly requires (by an internal memo signed by the CEO) that staff apply security requirements in accordance with the information security policy, specific policies and procedures established by the auditee.	➢ Internal note signed by the DG

1.2 Practical Application of Clause 5.4: Case Study: ”Tech Solutions”

The following document is an Internal Memorandum from the CEO of Tech Solutions to all employees. Its main purpose is to officially mandate that all personnel must comply with the company’s Information Security Policy, topic-specific policies, and established procedures:

TECH SOLUTIONS

Internal Memorandum

Subject: Mandatory Compliance with Information Security Policies and Procedures.

From: Mr. ……, Chief Executive Officer

To: All Tech Solutions Staff

Date: [Insert Date]

Dear Team,

At Tech Solutions, safeguarding information assets, particularly sensitive medical data and proprietary software, is fundamental to our business success and regulatory compliance.

In alignment with our Information Security Policy, specific policies, and established procedures, it is mandatory that all employees and contractors strictly adhere to these security requirements.

Management fully recognizes its responsibility to lead by example and expects each individual to:

- Understand and apply the information security policies relevant to their role.
- Respect confidentiality, integrity, and availability requirements for all information assets.

- Follow internal procedures, whether working from the office or remotely.
- Maintain an appropriate level of security awareness and skills through continuous learning.
- Promptly report any breaches or security incidents using the designated reporting channels.

We count on your full cooperation to protect the trust our clients place in us, meet our legal obligations (GDPR, HIPAA, ISO 27001, NIS 2), and maintain the high standards that define Tech Solutions.

Security is a shared responsibility, and your commitment is vital.
Strict compliance is non-negotiable.
Thank you for your continued support and dedication.

Sincerely,

Mr. .....
Chief Executive Officer
Tech Solutions

The following document is a formal statement from the CEO of Tech Solutions that outlines the company's commitment to information security:

TECH SOLUTIONS

MANAGEMENT COMMITMENT

To ensure its development and maintain technological excellence, Tech Solutions manages and protects critical informational assets shared with its clients (hospitals, private clinics, laboratories), partners, and suppliers. Our goal is to protect our clients' trust by securing sensitive information and ensuring the availability of our services, in compliance with international security standards.

Our ultimate objective is to safeguard our informational assets (medical data, source code, cloud platforms, etc.) against all threats, whether internal or external, deliberate or accidental, and thereby strengthen the trust of our clients and partners.

Tech Solutions' information security strategy is based on the following principles:

- Recognizing security as a core value, a driver of progress, and a measure of quality and efficiency.
- Ensuring the confidentiality, integrity, and availability of information, especially protected health data and source codes.
- Complying with internal security policies and external regulations, including GDPR, HIPAA, ISO 27001, and NIS 2.
- Meeting client requirements regarding cloud security, mobility, and secure software development (DevSecOps).
- Promoting security across all our activities, including remote work and the management of our physical and cloud infrastructures.

To achieve these goals, we have established an Information Security Management System (ISMS) in accordance with the ISO/IEC 27001:2022 standard.

As the Chief Executive Officer of Tech Solutions, I personally commit to:

- Supporting information security initiatives at all levels of the organization.
- Providing the human, financial, organizational, and technical resources necessary for the implementation and continuous improvement of the ISMS.
- Fostering a security culture among all employees, regardless of their role.

Aware that information security is everyone's responsibility, I rely on the active involvement of all staff members to ensure the success of this endeavor.

Mr. [Chief Executive Officer's Name]

Tech Solutions

[Physical Address]

[Phone Number] – [Email Address] – [Website URL]

1.3 Contact with authorities (5.5)

Control 5.5:

The organization should establish and maintain contact with relevant authorities.

Control attributes:

- Control type: When it acts : Preventive, corrective
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Identify, Protect, Respond, Recover
- Optional capabilities: Which operational area it belongs to : Governance
- Security domains: Which domain it relates to : Defence, Resilience

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Preventive Corrective	Confidentiality Integrity Availability	#Identify #Protect #Respond #Recover	Gouvernance	#Defence #Resilience

Control description:

The organization must clearly decide:

- Who will contact authorities (like the police, regulators, or supervisors),
- When to contact them,
- How to report any security incidents quickly.

The organization should also stay in touch with authorities to:

- Understand what rules and expectations apply now,
- Stay updated on any new regulations coming soon.

➔ You need a plan for communicating with outside authorities both when incidents happen and to keep informed about rules.

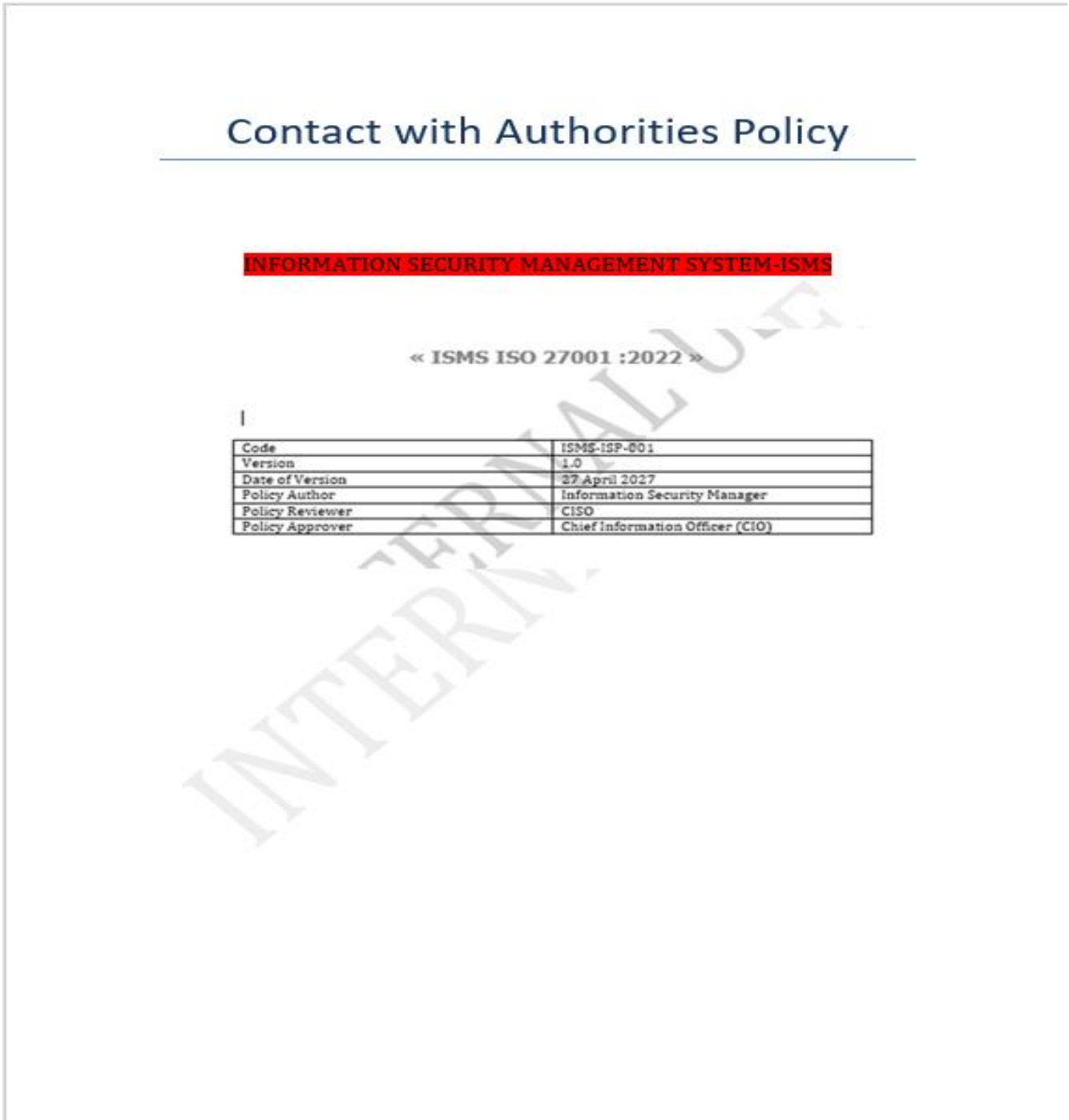
Control evidence:

Checks to be performed	Evidence
➢ Whether the authorities with which the organization can collaborate on information security matters are identified. ➢ Whether an updated contact list of these authorities is maintained. ➢ Whether a procedure for communication between the organization and these authorities is defined and implemented.	➢ Updated contact list of authorities with which the organization may collaborate, ➢ Procedure for communication between the organization and these authorities,

1.4 Practical Application of Clause 5.5: Case Study: ”Tech Solutions”

In alignment with ISO/IEC 27002:2022 Control 5.5, which emphasizes establishing and maintaining contact with relevant authorities, it's crucial for organizations to have a documented policy detailing these contacts. This ensures timely communication during information security incidents and compliance with legal and regulatory obligations.

Below is a document for a "Contact with Authorities" policy tailored for the organization “Terch Solution”:



Contact with Authorities Policy

INFORMATION SECURITY MANAGEMENT SYSTEM-ISMS

« ISMS ISO 27001 :2022 »

Code	ISMS-ISP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

Change History

Version	Date	Action	Created by
1.0	27 April 2025	Basic Document	Information Security Manager

1. Purpose

To establish and maintain appropriate contacts with relevant authorities to ensure effective communication during information security incidents, compliance with legal and regulatory requirements, and to stay informed about current and upcoming regulations.

2. Scope

This policy applies to all employees, contractors, and third-party users of [Organization Name] who are responsible for information security management and incident response.

3. Responsibilities

- Information Security Manager (ISM): Responsible for maintaining the contact list of relevant authorities and ensuring its accuracy.
- Incident Response Team (IRT): Responsible for communicating with authorities during information security incidents as per this policy.

4. Contact List of Relevant Authorities

Authority Name	Contact Person/Department	Contact Details	Purpose of Contact
Agence nationale de la sécurité des systèmes d'information (ANSSI)	CERT-FR	cert@ssi.gouv.fr +33 1 71 75 84 68	Reporting cybersecurity incidents, guidance on security measures
Commission Nationale de l'Informatique et des Libertés (CNIL)	Complaints Department	plainte@cnil.fr +33 1 53 73 22 22	Data protection compliance, reporting data breaches
Police Nationale – SCCCI	Investigation Unit	cybercrime@interieur.gouv.fr +33 1 40 07 60 60	Reporting cybercrimes, coordination during investigations
Gendarmerie Nationale – C3N	Specialized Unit	c3n@gendarmerie.interieur.gouv.fr +33 1 80 00 20 20	Reporting cyber incidents, collaboration on cybercrime cases
ARCEP	Network Security Directorate	securite@arcep.fr +33 1 40 47 70 00	Compliance with electronic communications regulations
Autorité des marchés financiers (AMF)	Legal Affairs Directorate	infosec@amf-france.org +33 1 53 45 60 00	Financial market regulations, reporting security incidents
Autorité de contrôle prudentiel et de résolution (ACPR)	On-Site Inspection Department	contact@acpr.banque-france.fr +33 1 49 95 40 00	Oversight of banking and insurance sectors

5. Procedures

- Regular Updates: The ISM shall review and update the contact list bi-annually or when significant changes occur.
- Incident Reporting: In the event of an information security incident, the IRT shall notify the relevant authority as per the contact list and document the communication.
- Training: Employees involved in incident response shall be trained on this policy and the procedures for contacting authorities.

6. Review and Maintenance

This policy shall be reviewed annually by the ISM and updated as necessary to reflect changes in legal requirements or organizational structure.

7. Approval

Approved by: [Name], [Title]

Date: [Date]

1.5 Contact with special interest groups (5.6)

Control 5.6:

The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations..

Control attributes:

- Control type: When it acts : Preventive, corrective
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Protect, Respond, Recover
- Optional capabilities: Which operational area it belongs to : Governance
- Security domains: Which domain it relates to : Defence

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Preventive Corrective	Confidentiality Integrity Availability	#Protect #Respond #Recover	Gouvernance	#Defence

Control description:

The organization should consider joining security-related groups or forums to:

- Learn and stay updated on best practices and new security info,
- Keep its knowledge of security threats and trends current,
- Get early warnings about cyberattacks or software fixes,
- Access expert security advice,
- Share and receive info on new tech, threats, or vulnerabilities,

Control evidence:

Checks to be performed	Evidence
➢ Whether interest groups, specialized security forums, and professional associations have been identified ➢ Whether contacts are established and maintained with these groups, forums, and associations ➢ Whether information-sharing agreements have been established to improve security cooperation and coordination	➢ Subscription ➢ Participation in workgroups ➢ Sharing feedback ➢ Agreements established with groups

1.6 Practical Application of Clause 5.6: Case Study: ”Tech Solutions”

The document titled "Subscription Agreement – Tech Solutions Ltd. and Information Security Forum (ISF)" is a professionally structured contract that formalizes the membership of Tech Solutions Ltd. in a special interest group (ISF):

SUBSCRIPTION AGREEMENT

Between Tech Solutions Ltd. and Information Security Forum (ISF)

1. PARTIES TO THE AGREEMENT

This Subscription Agreement is entered into as of April 28, 2025, by and between:
- Tech Solutions Ltd.
  Registered Address: 125 Innovation Park, Silicon Drive, NY, USA
  Represented by: James Donovan, Chief Information Security Officer (CISO)
  ("Subscriber")

and

- Information Security Forum (ISF)
  Registered Address: [Insert SIG Address]
  Represented by: [SIG Representative Name, Title]
  ("Provider")

2. PURPOSE

The Subscriber agrees to enroll in the Provider's special interest group membership, in support of its information security objectives to:
- Access expert information security guidance and research,
- Receive early alerts on vulnerabilities, threats, and best practices,
- Participate in forums and knowledge exchange,
- Strengthen its Information Security Management System (ISMS).

3. TERM & RENEWAL

Initial Term: One (1) year, from April 1, 2025 to March 31, 2026.
Renewal: Automatically renews annually unless terminated in writing 30 days prior to expiry.
Termination can be initiated by either party with prior notice.

4. FEES & PAYMENT

Annual Fee: USD 4,000
Payment Terms: Due within 30 days of invoice issuance.
Payment Method: Bank transfer to Provider's designated account.
Late payments may be subject to a 2% monthly interest charge.

5. MEMBER OBLIGATIONS

The Subscriber agrees to:
- Maintain an active designated contact person.
- Use the membership access exclusively for authorized personnel.
- Follow all confidentiality and usage policies of the Provider.
- Actively participate in relevant activities (e.g. webinars, forums).

6. PROVIDER OBLIGATIONS

The Provider agrees to:
- Grant access to exclusive resources and security research.
- Provide timely advisories, threat alerts, and vulnerability updates.
- Facilitate engagement through forums, webinars, and working groups.
- Ensure secure and confidential handling of Subscriber's data.

7. CONFIDENTIALITY

Both parties agree to maintain strict confidentiality regarding all sensitive, proprietary, or technical information exchanged during the term of this Agreement. This obligation continues after the Agreement ends.

8. TERMINATION

Either party may terminate this Agreement with 30 days' written notice. Refunds will not be issued for the unused portion of the membership unless the termination is due to a breach by the Provider.

9. GOVERNING LAW

This Agreement shall be governed by the laws of the State of New York, USA, unless otherwise agreed in writing.

10. SIGNATURES

For Tech Solutions Ltd.
Name: James Donovan
Title: Chief Information Security Officer (CISO)
Signature: _____
Date: April 28, 2025

For Information Security Forum (ISF)
Name: [SIG Representative Name]
Title: [Title]
Signature: _____
Date: April 28, 2025

The following document titled "Participation Evidence – Security Workgroups" is a formal record created by Tech Solutions Ltd. to demonstrate its active involvement in an external cybersecurity workgroup:

TECH SOLUTIONS

WORKGROUP PARTICIPATION FEEDBACK REPORT

Date of Submission: April 28, 2025

1. WORKGROUP OVERVIEW

Workgroup Title: Cloud Security and Threat Intelligence Workgroup
Organized By: Information Security Forum (ISF)
Meeting Date: April 22, 2025
Location: Virtual Meeting (Zoom Platform)
Duration: 2 Hours
Representative: Sarah Blake, Information Security Manager, Tech Solutions Ltd.

2. PURPOSE OF ATTENDANCE

The objective of attending this session was to stay informed on current cloud security risks, share experiences related to vulnerability management, and collaborate with peers on strategies to enhance threat detection and response mechanisms.

3. SUMMARY OF DISCUSSIONS

Key topics covered in the workgroup session included:
- Emerging threats in multi-cloud environments
- Best practices in cloud misconfiguration prevention
- Review of the latest threat intelligence reports
- Case study: Response to Log4Shell-type vulnerabilities
- Early warning systems and automation in threat detection

4. TECH SOLUTIONS' CONTRIBUTIONS

Tech Solutions Ltd., represented by Sarah Blake, actively participated by:
- Sharing internal strategies for cloud asset inventory and real-time alerting.

- Providing feedback on the effectiveness of current SIEM integrations.
- Engaging in Q&A on third-party risk monitoring tools.

5. ACTIONABLE TAKEAWAYS

Following outcomes will be explored for implementation:
- Reviewing internal cloud security posture using the shared checklist.
- Evaluating feasibility of adopting automated remediation for common misconfigurations.
- Subscribing to recommended open-source threat feeds discussed in the session.

6. ALIGNMENT WITH ISMS OBJECTIVES

This participation supports Tech Solutions' ISMS by improving real-time threat awareness, fostering collaboration, and aligning internal practices with industry benchmarks, in accordance with ISO/IEC 27002:2022 Clause 5.6.

7. APPROVAL

Approved by: James Donovan
Title: Chief Information Security Officer (CISO)
Signature: _____
Date: April 28, 2025

1.7 Threat intelligence (5.7)

Control 5.7:

Information relating to information security threats should be collected and analysed to produce threat intelligence.

Control attributes:

- Control type: When it acts : Preventive, detective, Corrective
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Identify, detect, Respond
- Optional capabilities: Which operational area it belongs to : Threat_and_vulner-ability_management
- Security domains: Which domain it relates to : Defence, Resilience

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Preventive Detective Corrective	Confidentiality Integrity Availability	#Identify #Detect #Respond	#Threat_and_vulner- ability_management	#Defence #Resilience

Control description:

The organization should gather and study information about security threats (like hackers, malware, or scams) so that you can:

- Take action to stop threats before they cause harm.
- Lessen the damage if threats do happen.

Control evidence:

Checks to be performed	Evidence
➢ Whether the internal and external information sources required for generating threat intelligence are identified ➢ Whether information on existing and emerging threats is collected, analyzed, communicated to the appropriate people, and used ➢ Whether the information collected from threat intelligence sources is integrated into the organization's information security risk management processes.	➢ List of threat intelligence sources ➢ Subscriptions and contracts with threat intelligence providers ➢ A sample of threat intelligence.

1.8 Practical Application of Clause 5.7: Case Study: ”Tech Solutions”

The Threat Intelligence Procedure for Tech Solutions Ltd. outlines how the company systematically gathers, processes, analyzes, and uses threat intelligence to improve its cybersecurity posture:

TECH SOLUTIONS

Threat Intelligence Procedure

« ISMS ISO 27001 :2022 »

Code	ISMS-ISP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

Change History

Version	Date	Action	Created by
1.0	27 April 2025	Basic Document	Information Security Manager

1. PURPOSE

This procedure outlines how Tech Solutions Ltd. collects, processes, analyzes, and uses threat intelligence to support proactive security measures and informed decision-making, in alignment with ISO/IEC 27002:2022 Clause 5.7.

2. SCOPE

This procedure applies to all departments and systems within Tech Solutions Ltd. where threat intelligence can enhance information security practices, including IT, Risk Management, and Executive Management.

3. DEFINITIONS

- Threat Intelligence: Information about threats and threat actors that helps an organization prevent or respond to cybersecurity incidents.
- IOCs (Indicators of Compromise): Technical evidence of potential or actual unauthorized system access.
- TTPs (Tactics, Techniques, and Procedures): Behavior patterns used by threat actors.

4. RESPONSIBILITIES

- IT Security Team: Collects and analyzes technical threat intelligence.
- Risk Management Team: Evaluates business impact of identified threats.
- CISO: Oversees program implementation and ensures continuous improvement.

5. PROCEDURE

5.1 Establish Threat Intelligence Objectives

Define what kind of intelligence is needed (strategic, tactical, operational) and how it will support risk management and technical defenses.

5.2 Identify and Vet Sources

Use both internal and external sources:
- Internal: SIEM logs, incident reports, vulnerability scans

- External: ISF, US-CERT, commercial feeds, security forums
Sources are reviewed quarterly for relevance and reliability.

5.3 Collect Threat Information

Threat information is collected continuously using automated tools (e.g., threat intelligence platforms, log aggregators) and manually during meetings or briefings.

5.4 Process and Normalize Data

Translate, clean, and format threat data for consistency. Use correlation tools to match external data with internal logs.

5.5 Analyze Threat Data

Determine the relevance, likelihood, and potential impact of threats. Classify threats as strategic, tactical, or operational. Use analytical tools and human review.

5.6 Distribute and Act on Intelligence

Share findings with:
- IT for control updates (e.g., blocklists, rules)
- Risk Management for risk scoring
- Executives for awareness

Use intelligence to adjust detection tools, incident response plans, and patching schedules.

5.7 Review and Improve

Conduct monthly reviews of intelligence processes and feedback from users. Update sources, tools, and reporting formats as needed.

6. RECORDS

- Threat intelligence summaries
- Source validation logs
- Intelligence dissemination logs
- Risk assessment updates linked to threat intelligence

7. APPROVAL

Approved by: James Donovan
Title: Chief Information Security Officer (CISO)
Signature: _____
Date: April 28, 2025

The following represent the list of Threat Intelligence Source:

TECH SOLUTIONS

List of Threat Intelligence Sources

« ISMS ISO 27001 :2022 »

Code	ISMS-ISP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

Change History

Version	Date	Action	Created by
1.0	27 April 2025	Basic Document	Information Security Manager

1. INTRODUCTION

This document outlines the internal and external sources used by Tech Solutions Ltd. to collect threat intelligence. These sources are essential for identifying, assessing, and responding to current and emerging cybersecurity threats.

2. INTERNAL SOURCES

Internal sources are derived from systems, processes, and activities within Tech Solutions Ltd. These provide contextual and operational data unique to our environment.

- SIEM Logs (Security Information and Event Management)
- Firewall and IDS/IPS logs (e.g., Palo Alto Networks, Snort)
- Endpoint Detection & Response (EDR) data
- Vulnerability management reports (e.g., Nessus, Qualys)
- Incident response reports
- Internal penetration testing and red team assessments
- Helpdesk tickets flagged as security-related
- User behavioral analytics (UBA) alerts

3. EXTERNAL SOURCES

External sources include public, commercial, governmental, and industry-specific feeds that provide broader visibility into the global threat landscape.

- 3.1 Open Source Intelligence (OSINT)

- US-CERT Alerts (https://www.cisa.gov/uscert)
- NIST National Vulnerability Database (https://nvd.nist.gov/)
- MITRE ATT&CK Framework (https://attack.mitre.org/)
- VirusTotal (https://www.virustotal.com/)
- AbuseIPDB (https://www.abuseipdb.com/)
- Shodan (https://www.shodan.io/)

- 3.2 Commercial Threat Intelligence Providers

- Recorded Future
- Mandiant Threat Intelligence
- IBM X-Force Exchange
- Anomali ThreatStream
- Cisco Talos Intelligence Group
- CrowdStrike Intelligence

- 3.3 Government and Law Enforcement

- ENISA (European Union Agency for Cybersecurity)
- NCSC (UK's National Cyber Security Centre)
- FBI InfraGard
- Europol EC3 (European Cybercrime Centre)

- 3.4 Industry Groups and ISACs (Information Sharing and Analysis Centers)

- FS-ISAC (Financial Services)
- IT-ISAC (Information Technology)
- Healthcare ISAC
- Local/national CERTs
- Tech Solutions participation in regional cybersecurity working groups

- 3.5 Social Media and Security Communities

- Twitter accounts of key security researchers and vendors
- Reddit (r/netsec, r/cybersecurity)
- LinkedIn professional threat intelligence groups
- Discord/Slack communities for threat sharing

4. SOURCE REVIEW AND VALIDATION

All sources are evaluated quarterly by the Threat Intelligence Team for relevance, timeliness, and reliability. Sources that consistently produce actionable intelligence are prioritized. New sources are vetted before integration into the threat intelligence platform.

5. APPROVAL

Approved by: James Donovan
Title: Chief Information Security Officer (CISO)
Signature: _____
Date: April 28, 2025

The following document represent a sample of threat intelligence :

TECH SOLUTIONS

Threat Intelligence Report

Company: Tech Solutions Ltd.

Prepared by: [Your Name/Position]

Date: April 29, 2025

1. Introduction

This document outlines the threat intelligence framework established by Tech Solutions to comply with ISO/IEC 27002:2022 Clause 5.7. The clause emphasizes the need for gathering, analyzing, and using threat intelligence to protect organizational assets and support informed decision-making.

2. Purpose

The purpose of this threat intelligence report is to demonstrate how Tech Solutions monitors and responds to current and emerging threats in order to improve its overall security posture and reduce risk exposure.

3. Threat Intelligence Sources

Tech Solutions gathers intelligence from the following sources:

- - Commercial threat intelligence feeds (e.g., Recorded Future, Anomali)
- - Open-source intelligence (OSINT) platforms (e.g., MITRE ATT&CK, VirusTotal)
- - Government alerts and advisories (e.g., CISA, ENISA)
- - Internal logs and SIEM data
- - Industry Information Sharing and Analysis Centers (ISACs)

4. Threat Intelligence Process

The following steps are taken to manage threat intelligence:

1. 1. Collection – Automated tools and analysts collect raw data.
2. 2. Processing – Data is cleaned and structured.
3. 3. Analysis – Analysts identify patterns and assess impact.
4. 4. Dissemination – Relevant intelligence is shared with stakeholders.
5. 5. Action – Security measures are updated based on insights.

5. Application and Use

Threat intelligence is integrated into the risk management, incident response, and vulnerability management programs. Real-time alerts enable proactive measures, such as IP blocking, patching, and communication with third parties.

6. Review and Update

This threat intelligence framework is reviewed quarterly and after major security events to ensure continued relevance and effectiveness.

7. Conclusion

Tech Solutions is committed to maintaining a robust threat intelligence program that meets ISO/IEC 27002 Clause 5.7 requirements, protecting its assets and supporting a secure operational environment.

8. Threat List

Below is a list of threats relevant to Tech Solutions' operational environment:

- Phishing attacks targeting employee credentials.
- Ransomware attacks impacting operational continuity.
- Supply chain attacks via third-party software providers.
- Zero-day vulnerabilities in web-facing applications.
- Insider threats from disgruntled or negligent employees.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
- Exploitation of misconfigured cloud resources.
- Credential stuffing attacks against user portals.
- Advanced Persistent Threats (APTs) from state-sponsored actors.
- Data exfiltration through malware or unauthorized access.

1.9 Information security in project management (5.8)

Control 5.8:

Information security should be integrated into project management.

Control attributes:

- Control type: When it acts : Preventive
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Identify, protect
- Optional capabilities: Which operational area it belongs to : Governance
- Security domains: Which domain it relates to : Governance_and_Ecosys-tem, Protection

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Preventive	Confidentiality Integrity Availability	#Identify #Protect	#Governance	#Governance_and_Ecosys-tem #Protection

Control description:

Whenever the organization runs a project (e.g., launching a new app, updating a system, or working with a vendor), you should think about information security from the beginning and continue to manage it until the project ends.

At the very beginning of a project, ask: “What could go wrong with our data or systems?”

As the project moves forward, keep reviewing those risks — not just once at the start.

List all security requirements from day one

For example:

- Does the app need strong password protection?
- Do you need to protect copyrighted materials?

Control evidence:

Checks to be performed	Evidence
➢ Whether an information security risk analysis is performed early in the project to identify necessary security controls and then periodically as project risks throughout the project lifecycle ➢ Whether information security requirements are determined for all types of projects	➢ Project documents containing the expression of security needs ➢ Information security project management procedure ➢ Risk analysis document

1.10 Practical Application of Clause 5.8: Case Study: ”Tech Solutions”

This Information Security Checklist for Project Management provides a simple, actionable guide to help project managers meet the requirements of ISO/IEC 27002:2022, specifically those related to incorporating security throughout the project lifecycle:

Information Security Checklist for Project Management

Date: April 29, 2025

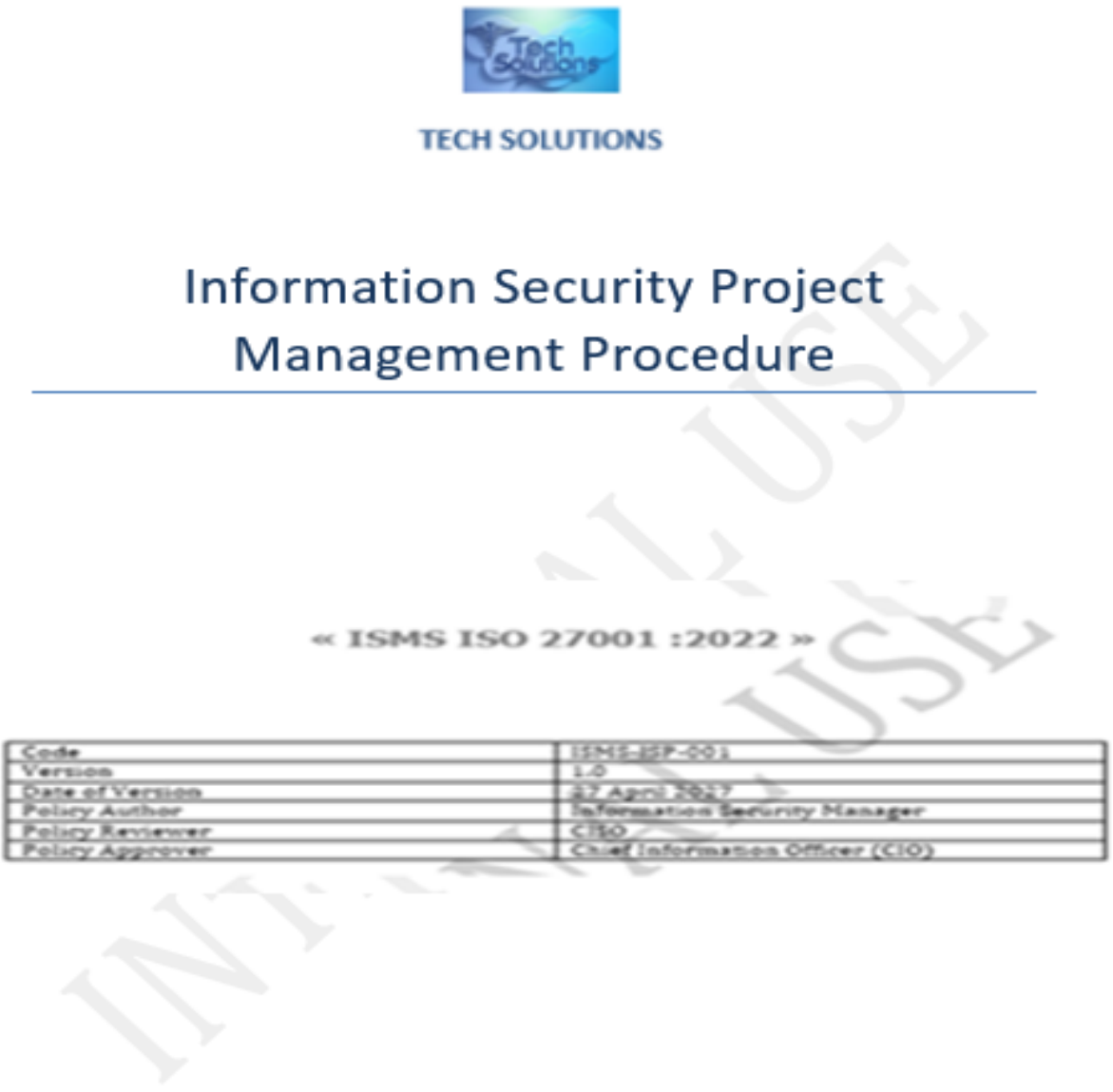
Purpose

This checklist is designed to help project managers at Tech Solutions ensure that information security is considered throughout the project lifecycle, in alignment with ISO/IEC 27002:2022 requirements.

Checklist for Project Managers

- Have you identified potential information security risks at the start of the project?
- Are these risks being reviewed and updated regularly throughout the project?
- Have you defined all relevant information security requirements early in the project (e.g., data protection, access control, IP rights)?
- Have you ensured that secure communication methods are in place for both internal and external communication?
- Are you continuously monitoring and addressing new security risks as the project progresses?
- Are measures in place to treat (reduce/mitigate) the identified risks?
- Is there a clear plan to track the progress of risk treatment actions?
- Have you tested the effectiveness of the risk treatment measures (e.g., penetration tests, vulnerability scans)?
- Are all stakeholders aware of their roles in ensuring project security?
- Is security documented and included in project reporting and updates?

The Information Security Project Management Procedure for Tech Solutions outlines how the organization ensures that information security is embedded throughout all project phases—from planning to completion:



TECH SOLUTIONS

Information Security Project Management Procedure

« ISMS ISO 27001 :2022 »

Code	ISMS-SPP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

Change History

Version	Date	Action	Created by
1.0	27 April 2025	Base Document	Information Security Manager

1. Purpose

This procedure ensures that all projects at Tech Solutions are managed in a manner that safeguards the confidentiality, integrity, and availability of information assets. It aligns with ISO/IEC 27001:2022 and supports compliance with legal and regulatory requirements, including GDPR and HIPAA.

2. Scope

This procedure applies to all projects at Tech Solutions that may affect the organization's information security. This includes projects related to software development, cloud infrastructure, internal systems, and client services.

3. Responsibilities

- The Information Security Manager is responsible for oversight and compliance monitoring.
- Project Managers are responsible for integrating security controls into their project plans.
- Project Team Members must follow all security-related instructions and report issues.

4. Integration of Security in the Project Lifecycle

- Security requirements must be identified and documented in the early stages of all projects.
- Risk assessments must be conducted to identify potential threats to data, systems, and users.
- Security controls and mitigation strategies must be planned, implemented, and monitored.
- Regular reviews of risk treatment progress and effectiveness must be performed.

5. Access Control and Authorization

- Access to project data must be granted on a need-to-know and least privilege basis.
- Multi-factor authentication (MFA) must be used for accessing sensitive project resources.
- Access permissions must be reviewed regularly and revoked when no longer required.

6. Monitoring and Evaluation

- Security performance must be monitored throughout the project.
- Any incidents must be reported and managed according to the incident response plan.
- Project audits must be conducted to verify compliance with security requirements.

7. Training and Awareness

• All project participants must receive training on relevant information security policies.
• Ongoing awareness campaigns should reinforce best practices and organizational expectations.

8. Documentation and Traceability

• All security-related project activities must be documented and stored securely.
• Documentation should provide traceability for decisions, controls, and incidents.

9. Procedure Review

This procedure shall be reviewed annually or after significant changes to ensure continued relevance and effectiveness.

10. Non-Conformity

Any deviation from this procedure not formally approved by the Information Security Manager will be considered a non-conformity and may result in disciplinary action.

1.11 Inventory of information and other associated assets (5.9)

Control 5.9:

An inventory of information and other associated assets, including owners, should be developed and maintained.

Control attributes:

- Control type: When it acts : Preventive
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Identify
- Optional capabilities: Which operational area it belongs to : Asset_management
- Security domains: Which domain it relates to : Governance_and_Ecosys-tem, Protection

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Preventive	Confidentiality Integrity Availability	#Identify	#Asset_manage- ment	#Governance_and_Ecosys- tem #Protection

Control description:

Organization wants to:

- Know what assets you have
- Understand how important they are
- Keep track of them accurately
- Assign responsibility to someone for each asset

You should:

- Find out what assets (like data, software, servers, laptops, etc.) your organization uses.
- Understand how important each one is for security (e.g., is it confidential, critical for business, etc.).
- Keep a list (inventory) of these assets.

Make sure: The inventory is correct, up-to-date, and doesn't contradict other records.

You can keep separate lists, like:

- One for hardware (laptops, phones)
- One for software
- One for information (documents, databases)
- One for people (who has what access, etc.)
- One for virtual machines, etc.

Use labels (like “Confidential”, “Internal”, “Public”) to show how sensitive the asset is — based on the information it handles.

Every asset (like a database, a server, a set of files) should have a responsible person or team.

Update the owner if the responsible person leaves or changes role.

The owner must: a) Make sure the asset is in the inventory

b) Make sure it’s properly classified and protected

c) Review the classification over time

d) List related components (e.g., what software or databases are part of a system)

e) Define rules for how people can use the asset (e.g., no personal use)

f) Set and review access controls based on sensitivity

g) Ensure secure deletion or disposal and remove it from the inventory

h) Help identify and manage risks related to the asset

Control evidence:

Checks to be performed	Evidence
➢ Whether asset inventory procedures are developed ➢ Whether an inventory or register is maintained for the assets and whether their importance in terms of information security is determined ➢ Whether asset ownership is assigned to a person or group for the identified information and other associated assets	➢ Inventory procedure ➢ Inventory of information and other associated assets

1.12 Practical Application of Clause 5.9: Case Study: ”Tech Solutions”

Asset Category & Criticality :

Asset Category	Asset	Owner	Asset Code	Criticality Level	Confidentiality	Integrity	Availability	Status	Location
Hardware	Virtualization Servers	Infrastructure Team	MAT-INF	High	High	High	High	Active	Primary Data Center
Hardware	Employee Laptops	HR Department	MAT-INF	Medium	Medium	Medium	High	Active	Corporate Offices
Network	Core Switch	Network Operations	SW	High	Medium	High	High	Active	Main Network Hub
Process	Service Desk Ticketing	ITSM Team	P.M	High	High	High	High	Active	ITSM Platform
Process	Data Backup and Archiving	Infrastructure Team	A	High	High	High	High	Active	Backup Data Center
Software	Customer Support CRM	Customer Success	APP	High	High	High	Medium	Active	CRM Cloud
Software	ERP System	Finance Department	PROGL	High	High	High	Medium	Active	ERP Cloud
Software	Firewall Control Software	Security Team	EQ-Sec	High	High	High	High	Active	Firewall Cluster
Network	Corporate LAN	Network Operations	PA	High	Medium	High	High	Active	HQ LAN
Network	Remote VPN Access	IT Security	PA	High	Medium	High	High	Active	VPN Gateway
Network	Wireless Infrastructure	Network Operations	SW	High	Medium	Medium	High	Active	Wireless Access Points
Personnel	System Administrator	Infrastructure Team	EXP	High	High	High	High	Active	Admin Office
Personnel	Cybersecurity Engineer	Security Team	EXP	High	High	High	High	Active	Security Operations
Personnel	Recruitment Officer	HR Department	DIR	Medium	Medium	Medium	Medium	Active	HR Wing
Site	Headquarters	Facilities	LOC	High	Low	Medium	High	Active	Tech HQ
Site	Cloud Hosting Region	Cloud Services	LOC	High	High	High	High	Active	Cloud Provider
Site	Remote Office	Operations	LOC	Medium	Low	Medium	High	Active	Branch Office

Asset valuation table :

Level	Asset Value	Definition
5	Critical	Asset essential to company operations. Unavailability causes total business halt or major damage (legal, financial, reputation).
4	Very Important	Asset required by multiple departments or major processes. Its loss significantly degrades business performance.
3	Important	Useful for regular operations, but loss does not stop critical functions. Localized or time-limited impact.
2	Low	Secondary or easily replaceable asset. Minor and limited impact if unavailable.
1	Negligible	Non-strategic asset. Loss has little to no impact.

Identification Of Assets

Business Process	Confidentiality	Integrity	Availability
Client Onboarding	3	3	4
Incident Management	2	4	4
Vulnerability Management	4	4	3
Monthly Payroll	4	4	2
Customer Support	3	3	4
New Employee Provisioning	2	3	3
Data Backup	2	4	4
Software Deployment	2	3	3
Financial Reporting	4	4	2
Access Management	4	4	3
Change Management	3	4	3
Cloud Resource Monitoring	2	3	4
Remote Access Management	4	3	4

Information assets

Process	Type of Information Asset	Information Asset	Classification	Confidentiality	Integrity	Availability
Client Data Management	Database	Customer Medical Data	High	4	4	3
Medical Platform Access	Application	Online Medical Platform	High	3	4	4
Cloud Service Provisioning	Infrastructure	Cloud Hosting Environment	High	3	4	4
Billing and Invoicing	Application	Financial System	Medium	3	4	3
Remote Work Access	Infrastructure	VPN and Remote Desktop	High	3	3	4
Software Development	Code Repository	Medical App Source Code	High	4	4	3
Recruitment and Onboarding	Document Repository	Employee Files	Medium	3	3	2
Customer Support	Application	CRM System	Medium	3	3	3
E-commerce Transactions	Application	E-commerce Website	High	3	4	4
Development Operations	Server	Internal Development Servers	Medium	2	3	3
Data Backup	Infrastructure	Backup Systems (On-site and Cloud)	High	2	4	4
Regulatory Compliance Monitoring	Document Repository	Compliance Reports and Logs	High	4	4	2
Mobile Device Access	Device	Laptops and Mobile Phones	Medium	3	3	3
Physical Access Control	Infrastructure	Office and Data Center Access Systems	High	2	4	4
Marketing Campaigns	Application	Marketing Platform	Low	2	2	3

Hardware assets

Hardware Asset	Type	Confidentiality	Integrity	Availability
Internal Development Servers	Server	3	4	3
Cloud Hosting Servers	Cloud Infrastructure	4	4	4
Employee Laptops	Workstation	3	3	3
Firewall Appliance	Security Hardware	4	4	4
Wi-Fi Routers	Networking Equipment	2	3	3
VPN Gateway Device	Security Appliance	4	3	4
NAS Backup System	Storage	3	4	4
Access Control Panel	Physical Security Device	2	2	3
Network Switches	Networking Equipment	2	3	4
Mobile Devices (Remote Staff)	Portable Device	3	2	3
Physical Office Servers	On-site Server	3	4	3
Development Test Machines	Workstation	2	3	2

Application asset

Application	Application Type	Confidentiality (1-4)	Integrity (1-4)	Availability (1-4)
Online Medical Platform	Web Application	4	4	4
Customer Database	Database	4	4	4
Billing and Payments System	Financial Application	4	4	3
Internal Development Server	Server Application	3	4	3
E-commerce Website	Web Application	3	3	4
Client Cloud Hosting	Cloud Infrastructure	4	4	4
Source Code Repository	Development Tool	4	4	3
Internal Communication Tool	Collaboration Software	3	3	3
Remote Access VPN	Security Tool	4	4	4
HR Management System	Administrative Application	3	3	2
Monitoring and Logging Tools	Infrastructure Tool	2	3	4
Backup and Recovery System	Infrastructure Tool	3	4	4

Supplier asset

Supplier	Type of Supplier	Classification (1=Low, 4=Critical)
Cloud Provider X	Cloud Infrastructure	4
Medical API Provider	Medical Data Integration	4
Secure Email Service	Communication Service	3
Payment Gateway Provider	Financial Transaction Processor	4
IT Equipment Vendor	Hardware Supplier	2
Software License Vendor	Development Tools	3
Remote Access Platform Vendor	Remote Work Tools	3
Security Consultancy	Compliance and Audit Partner	4
Internet Provider	Network and Connectivity	3
External Data Center	Hosting Facility	4
Cleaning and Maintenance Contrac	Facility Service	1
Backup Service Provider	Data Backup and Recovery	4
CRM Vendor	Customer Management Tools	3

Personnel asset

Supplier	Type of Supplier	Classification (1=Low, 4=Critical)
Cloud Provider X	Cloud Infrastructure	4
Medical API Provider	Medical Data Integration	4
Secure Email Service	Communication Service	3
Payment Gateway Provider	Financial Transaction Processor	4
IT Equipment Vendor	Hardware Supplier	2
Software License Vendor	Development Tools	3
Remote Access Platform Vendor	Remote Work Tools	3
Security Consultancy	Compliance and Audit Partner	4
Internet Provider	Network and Connectivity	3
External Data Center	Hosting Facility	4
Cleaning and Maintenance Contrac	Facility Service	1
Backup Service Provider	Data Backup and Recovery	4
CRM Vendor	Customer Management Tools	3