ISO/IEC 27002:202

Mastering the Essentials of Information Security Controls

Your Practical Path to ISO/IEC 27001 Certification

Avoid Minor and Major Non-Conformities

Learn by Doing: Practical Guide

Noureddine Kanzari

Part 5

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 4

1.1 Monitoring, review and change management of supplier services (5.22) 4

1.2 Practical Application of Clause 5.22: Case Study: ”Tech Solutions” 8

1.3 Information security for use of cloud services (5.23) 19

1.4 Practical Application of Clause 5.23: Case Study: ”Tech Solutions” 22

1.5 Information security incident management planning and preparation (5.24) 38

1.6 Practical Application of Clause 5.24: Case Study: ”Tech Solutions” 42

1. ORGANIZATIONAL CONTROLS

1.1 Monitoring, review and change management of supplier services (5.22)

Control 5.22:

The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

Control attributes:

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

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventive	Confidentiality Integrity Availability	Identify	Supplier_relation- ships_security	#Governance_and_ Ecosystem #Protec- tion #Defence #Information_secu- rity_assurance

Control description:

- Regularly check if the supplier is delivering services especially regarding security. (Example: You hire a cloud storage provider to store your company's data securely. The contract says they must have 99.9% uptime and encrypt all data. You check their monthly performance reports to confirm they're meeting these standards: Review reports, dashboards, or metrics the supplier provides.)
- Check if the supplier improves their services in ways that could affect security. (Example: Your email service provider adds a new feature like AI-based spam filtering.

You need to confirm this doesn't weaken security. Ask the supplier to notify you about new features and review their impact on security)

- Ensure any new software or systems the supplier builds don't introduce security risks. (Example: Your supplier creates a new customer portal. You check if it's secure against hacking. Request details about new systems and verify they meet security standards)
- Make sure changes to the supplier's internal rules don't weaken security. (Example: The supplier updates their password policy to allow weaker passwords. You need to catch this and discuss it. Review their updated policies during meetings or audits)
- Check if the supplier adds or changes security measures (like firewalls) to fix issues or improve protection. (Example: After a data breach, the supplier adds two-factor authentication. You verify it's implemented correctly. Ask for details on new security controls and test them if possible)
- Ensure network upgrades don't create vulnerabilities. (Example: The supplier upgrades their Wi-Fi network. You check if it's still encrypted and secure. request network change reports and review them)
- Make sure new tech doesn't introduce risks. (Example: The supplier starts using a new cloud platform. You confirm it's certified for security. Ask about new tech and check its security certifications)
- Verify that new software versions are secure. (Example: The supplier upgrades their antivirus software. You ensure it's still effective against threats. Review release notes or test the new version)
- Ensure moving offices or data centers doesn't affect security. (Example: The supplier moves their data center to a new city. You check if the new location has proper security (like guards or cameras). Request details about the new location and its security measures.
- Make sure new subcontractors meet security standards. (Example: Your supplier hires a new company to handle backups. You verify they're secure. Review the sub-supplier's credentials and security practices)
- Regularly read reports from the supplier and meet to discuss performance and issues. (Example: The supplier sends a monthly report showing system uptime and security incidents. You meet quarterly to discuss trends and concerns. Schedule meetings and ask for specific reports to review)
- Check the supplier's and their subcontractors' security practices, using your own audits. (Example: You visit the supplier's office to check their security setup or review a third-party audit report showing they're compliant. Plan audits, review reports, and follow up on any issues found)
- Share and discuss details of security incidents as required by the contract. (Example: The supplier reports a phishing attack. You review how they handled it and ensure it won't happen again. Set up a process for incident reporting and review)

- Check logs and records of security events, problems, or disruptions to ensure the supplier is managing them well. (Example: You review logs showing a server crash to confirm the supplier fixed it quickly and securely. Ask for access to logs and analyze them regularly)
- Act quickly to handle any security issues with the supplier. Example: If the supplier's system is hacked, you work with them to contain the breach and prevent future attacks. Have an incident response plan and coordinate with the supplier)
- Find weaknesses in the supplier's systems and fix them. (Example: A security scan shows the supplier's software has a vulnerability. You ask them to patch it immediately. Use tools to scan for vulnerabilities and follow up on fixes)
- Confirm the supplier has plans to keep services running during crises (like power outages or natural disasters). (Example: The supplier's data center floods. You verify they have a backup center to keep your data accessible. Review their business continuity and disaster recovery plans)
- The supplier should have someone responsible for following the contract's security rules. (Example: The supplier appoints a security officer to handle your contract. You meet them to discuss compliance. Confirm who's responsible and communicate with them regularly)
- Continuously check that the supplier maintains strong security. (Example: Every six months, you assess the supplier's security using a checklist to ensure they're still compliant. Use audits, reports, and tests to evaluate security)
- Appoint a person or team in your organization to manage the supplier relationship. They need enough technical skills and tools to monitor security. (Example: You assign your IT manager to oversee the supplier. They use monitoring software to track performance and attend security training. Choose a qualified person, provide training, and give them tools like dashboards or audit software)
- If the supplier isn't meeting security or service standards, take steps to fix it. (Example: The supplier's uptime drops below the agreed level. You meet with them to discuss improvements or consider penalties. Document issues, discuss solutions with the supplier, and escalate if needed (e.g., contract termination)

Control evidence:

Checks to be performed	Evidence
➢ Whether service performance levels are monitored and whether their compliance with agreements is verified ➢ Whether service reports produced by the supplier are reviewed and regular progress meetings are held as required by the agreements ➢ Whether changes to agreements with suppliers are managed	➢ Supplier service performance level monitoring report ➢ Reports of changes made by the auditee ➢ Minutes of meetings with suppliers

TECH SOLUTIONS

Supplier Service Performance Level Monitoring Report

Organization: Tech Solutions
Report Period: Q1 2025 (January 1, 2025 – March 31, 2025)
Supplier: CloudSafe IT Services
Prepared by: Jane Doe, IT Security Manager
Date: April 10, 2025

---

1. Purpose

This report evaluates CloudSafe IT Services' performance against the terms of the supplier agreement, focusing on information security, service delivery, and compliance with ISO 27001 requirements. It covers service performance, changes in services, security incidents, and audit findings to ensure the supplier meets Tech Solutions' security and operational expectations.

---

2. Supplier Agreement Overview

Service Provided: Cloud storage and backup services
Key Contract Terms:

- 99.9% service uptime.
- Data encryption (AES-256) at rest and in transit.
- Incident response within 4 hours of detection.
- Quarterly security audits and reports.
- Notification of changes to services, subcontractors, or facilities within 5 business days.
- Maintain business continuity plans for major disruptions.

---

3. Service Performance Monitoring

Objective

Verify that CloudSafe IT Services meets the performance levels outlined in the agreement.

Metrics and Findings

Metric	Contract Target	Actual Performance	Compliance Status
Service Uptime	99.9%	99.92%	Compliant
Data Encryption Compliance	100% AES-256	100%	Compliant
Incident Response Time	Within 4 hours	Avg. 3.5 hours	Compliant
Backup Success Rate	100%	99.8% (1 failed backup, resolved)	Minor Non-Compliance

Comments

- Uptime exceeded the target, ensuring reliable access to services.
- One backup failure occurred due to a server glitch but was resolved within 24 hours. CloudSafe implemented a patch to prevent recurrence.

---

4. Monitoring Supplier Changes

Objective

Track changes made by CloudSafe IT Services to ensure they do not impact security or service delivery.

Changes Observed

Change Type	Details	Impact Assessment	Action Taken
Enhancements to Services	Added AI-based anomaly detection for backups.	Positive; improves security.	Reviewed feature documentation; confirmed compliance.
New Applications/Systems	Introduced a new user portal for backup management.	Potential risk; assessed for vulnerabilities.	Conducted security scan; no issues found.
Policy/Procedure Updates	Updated password policy to require 12 characters (previously 8).	Positive; strengthens security.	Verified policy alignment with Tech Solutions' standards.
New/Changed Security Controls	Implemented multi-factor authentication (MFA) for admin accounts.	Positive; enhances access control.	Tested MFA implementation; confirmed functionality.

Comments

- All changes were notified within the agreed 5-day period.
- Tech Solutions reviewed each change to ensure no negative impact on security or service delivery.

---

5. Monitoring Changes in Supplier Services

Objective

Evaluate changes to CloudSafe's infrastructure, tools, or business setup to ensure continued security and compliance.

Changes Observed

Change Type	Details	Impact Assessment	Action Taken
Network Enhancements	Upgraded to a new firewall system.	Positive; improves network security.	Reviewed firewall configuration; confirmed secure setup.
New Technologies	Adopted a new cloud orchestration tool (Kubernetes).	Neutral; assessed for risks.	Verified tool's security certifications.
New Product Versions	Upgraded backup software to version 3.2.	Neutral; checked for vulnerabilities.	Reviewed release notes; no security issues.
Development Tools	Switched to a new code repository (GitLab).	Neutral; assessed for security.	Confirmed secure access controls.
Physical Location Changes	None reported.	N/A	N/A
Change of Sub-Suppliers	Replaced backup tape vendor with a new provider.	Potential risk; assessed vendor.	Reviewed new vendor's security practices; compliant.
Sub-Contracting	None reported.	N/A	N/A

Comments

- All changes were documented and reviewed. No disruptions to service were noted.
- The new sub-supplier was audited to confirm compliance with security requirements.

---

6. Service Reports and Progress Meetings

Objective

Review CloudSafe's service reports and discuss performance in regular meetings.

Activities

- **Reports Reviewed**: Monthly uptime reports, quarterly security reports, and incident logs.
- **Meetings Held**: Quarterly progress meeting on March 15, 2025.
- **Key Discussion Points**:
  - Backup failure incident and resolution.
  - Implementation of MFA and its impact on security.
  - Upcoming plans for data center redundancy.

Comments

- Reports were timely and detailed, meeting contract requirements.
- Meetings provided clarity on performance and planned changes.

---

7. Audits and Follow-Ups

Objective

Conduct audits of CloudSafe and its sub-suppliers to verify compliance.

Audit Activities

- **Internal Audit**: Tech Solutions conducted a remote audit of CloudSafe's security controls on February 10, 2025.
- **Independent Audit**: Reviewed CloudSafe's SOC 2 Type II report (dated December 2024).
- **Sub-Supplier Audit**: Evaluated the new backup tape vendor's security practices.

Findings

- CloudSafe's controls were compliant with ISO 27001.
- Minor issue: One server lacked the latest security patch (resolved during audit).
- Sub-supplier met security standards.

Follow-Up Actions

- Confirmed patch deployment on all servers.
- Scheduled next audit for Q3 2025.

8. Security Incidents and Vulnerabilities

Objective

Monitor and manage security incidents and vulnerabilities.

Incidents Reported

Incident	Date	Description	Response Time	Resolution Status
Phishing Attempt	Jan 20, 2025	Unauthorized access attempt on backup portal.	3 hours	Resolved; MFA enforced.
Backup Failure	Feb 5, 2025	Server glitch caused one backup to fail.	4 hours	Resolved; patch applied.

Vulnerabilities Identified

- A vulnerability in the backup software (pre-version 3.2) was identified via a security scan.
- **Action**: CloudSafe upgraded to version 3.2, and Tech Solutions verified the fix.

Comments

- Incidents were handled within the agreed response time.
- Vulnerability management was proactive, with no exploitation reported.

---

9. Supplier's Sub-Supplier Relationships

Objective

Ensure CloudSafe's sub-suppliers meet security standards.

Findings

- CloudSafe uses one sub-supplier for backup tape storage.
- The new vendor was assessed and found compliant with ISO 27001 requirements.
- CloudSafe provided documentation of the vendor's security controls.

Comments

- No issues identified. Tech Solutions will include sub-supplier checks in future audits.

---

10. Service Continuity and Disaster Recovery

Objective

Verify CloudSafe's ability to maintain services during major disruptions.

Findings

- CloudSafe maintains a business continuity plan with a secondary data center.
- Tested failover to the secondary center during the February audit; completed successfully.
- Disaster recovery plan includes 24-hour recovery time objective (RTO), meeting contract terms.

Comments

- Continuity plans are robust and align with Tech Solutions' requirements.

---

11. Supplier Responsibilities and Compliance

Objective

Ensure CloudSafe assigns responsibilities for contract compliance.

Findings

- CloudSafe appointed a Security Officer (John Smith) to manage Tech Solutions' contract.
- The officer provided timely responses and coordinated audits and meetings.

Comments

- Clear responsibilities are in place, ensuring effective communication.

---

12. Ongoing Security Evaluation

Objective

Regularly assess CloudSafe's security levels.

Activities

- Quarterly security checklist completed.

- Penetration test conducted by Tech Solutions in March 2025; no critical issues found.
- Reviewed CloudSafe's ISO 27001 certification (valid until June 2026).

Comments

- CloudSafe maintains adequate security levels, with no major deficiencies.

---

13. Issues and Corrective Actions

Issue	Description	Corrective Action	Status
Backup Failure	One backup failed due to a server glitch.	Applied patch; added monitoring alert.	Resolved
Unpatched Server	One server lacked a security patch.	Deployed patch; updated patch management.	Resolved

---

14. Recommendations

1. Implement automated alerts for backup failures to reduce resolution time.
2. Schedule a joint tabletop exercise for disaster recovery in Q2 2025.
3. Request more frequent vulnerability scans (monthly instead of quarterly).

---

15. Conclusion

CloudSafe IT Services has largely complied with the supplier agreement and ISO 27001 requirements during Q1 2025. Minor issues (backup failure and unpatched server) were promptly resolved, and no significant security risks were identified. Tech Solutions will continue to monitor performance, changes, and security through reports, meetings, and audits.

Next Steps:

- Review Q2 2025 performance report (due July 10, 2025).
- Conduct follow-up audit in Q3 2025.
- Discuss recommendations in the next progress meeting (June 15, 2025).

Approved by:
Jane Doe, IT Security Manager
Tech Solutions

TECH SOLUTIONS

Minutes of Meeting with Supplier - Tech Solutions

Meeting Title: Quarterly Supplier Review Meeting
Date: May 5, 2025
Time: 10:00 AM - 11:30 AM
Location: Virtual (Zoom)
Attendees:

- **Tech Solutions**:
  - Jane Smith (IT Manager, Supplier Relationship Manager)
  - John Doe (Information Security Officer)
- **Supplier (CloudSafe Inc.)**:
  - Alice Brown (Account Manager)
  - Bob Wilson (Security Lead)

Purpose: To review CloudSafe Inc.'s service performance, compliance with the service agreement, security incidents, changes, and action plans as per ISO 27001 requirements.

Agenda

1. Review of Service Performance Levels
2. Discussion of Supplier Changes
3. Security Incidents and Vulnerabilities
4. Audit and Sub-Supplier Updates
5. Service Continuity and Compliance Responsibilities)
6. Action Items and Next Steps

---

1. Review of Service Performance Levels

- **Objective**: Verify compliance with the service agreement (uptime, response times, security controls).
- **Discussion**:
  - CloudSafe provided their Q1 2025 performance report, showing:
    - **Uptime**: 99.95% (meets agreement requirement of 99.9%).
    - **Incident Response Time**: Average of 2 hours (within 4-hour SLA).
    - **Data Encryption**: All data encrypted using AES-256 as agreed.
  - Jane Smith reviewed the report and confirmed metrics align with the contract.
  - Minor issue: One downtime event (15 minutes) due to server maintenance not pre-notified.
- **Action**:
  - CloudSafe to notify Tech Solutions at least 48 hours before planned maintenance.
  - Responsible: Alice Brown. Deadline: Ongoing.

---

2. Discussion of Supplier Changes

- **Objective**: Monitor changes in services, systems, or processes
- **Discussion**:
  - **Enhancements to Services (b1)**: CloudSafe introduced AI-based threat detection. Bob Wilson confirmed it's ISO 27001-compliant and enhances security.
  - **New Applications (b2)**: New backup management portal launched. Tech Solutions requested a security assessment report.
  - **Policy Updates (b3)**: CloudSafe updated their password policy to enforce 12-character minimums. John Doe confirmed this aligns with Tech Solutions' requirements.
  - **Network Changes (c1)**: CloudSafe upgraded to a new firewall system. No disruptions reported.
  - **New Technology (c2)**: Adoption of a new cloud orchestration tool. Bob Wilson shared its security certification (SOC 2).
  - **Location Change (c5)**: CloudSafe plans to relocate a secondary data center in Q3 2025.
  - **Sub-Supplier Change (c6, c7)**: CloudSafe switched to a new backup provider (BackupPro). Tech Solutions requested details on BackupPro's security practices.
- **Actions**:
  - CloudSafe to provide a security assessment for the new backup portal by May 15, 2025. Responsible: Bob Wilson.
  - CloudSafe to share details of the new data center's security measures by July 1, 2025. Responsible: Alice Brown.
  - CloudSafe to provide BackupPro's ISO 27001 certification or equivalent by May 20, 2025. Responsible: Alice Brown.

---

3. Security Incidents and Vulnerabilities

- **Objective**: Review incidents, vulnerabilities, and responses
- **Discussion**:
  - **Incidents (f, h)**: One phishing attempt detected in Q1 2025, mitigated within 1 hour. CloudSafe shared an incident report showing no data breach occurred.
  - **Vulnerabilities (i)**: A vulnerability scan identified a weak SSL configuration, patched in March 2025.
  - **Audit Trails (g)**: CloudSafe provided logs of the phishing incident and SSL patch. John Doe reviewed and found them satisfactory.
- **Action**:
  - CloudSafe to conduct a follow-up vulnerability scan by June 1, 2025, and share results. Responsible: Bob Wilson.

---

4. Audit and Sub-Supplier Updates

- **Objective**: Review audits and sub-supplier security
- **Discussion**:
  - **Audits (e)**: CloudSafe shared their 2024 ISO 27001 audit report, with no major non-conformities.
  - **Sub-Suppliers (j)**: BackupPro (new sub-supplier) is scheduled for an audit in Q2 2025. Tech Solutions requested to join the audit.
  - **Issues**: A minor audit finding (outdated access control list) was resolved in April 2025.
- **Actions**:
  - CloudSafe to invite Tech Solutions to BackupPro's audit. Responsible: Alice Brown. Deadline: June 15, 2025.
  - Tech Solutions to review the resolved audit finding's closure report by May 10, 2025. Responsible: John Doe.

---

5. Service Continuity and Compliance Responsibilities

- **Objective**: Ensure service continuity and compliance oversight
- **Discussion**:
  - **Continuity (k)**: CloudSafe's disaster recovery plan was tested in Q1 2025, with a recovery time of 4 hours (meets 6-hour SLA).
  - **Compliance (l)**: CloudSafe confirmed Bob Wilson as the security compliance lead for Tech Solutions' contract.
  - **Evaluation (m)**: Tech Solutions assessed CloudSafe's security levels as adequate based on reports and audits.
- **Action**:
  - CloudSafe to share the next disaster recovery test plan by August 1, 2025. Responsible: Bob Wilson.

---

6. Action Items and Next Steps

- **Summary of Actions**:
    1. CloudSafe to notify Tech Solutions before maintenance (Ongoing, Alice Brown).
    2. Provide security assessment for new backup portal (May 15, 2025, Bob Wilson).
    3. Share new data center security details (July 1, 2025, Alice Brown).
    4. Provide BackupPro's certification (May 20, 2025, Alice Brown).
    5. Conduct follow-up vulnerability scan (June 1, 2025, Bob Wilson).
    6. Invite Tech Solutions to BackupPro audit (June 15, 2025, Alice Brown).
    7. Tech Solutions to review audit finding closure (May 10, 2025, John Doe).
    8. Share disaster recovery test plan (August 1, 2025, Bob Wilson).
- **Next Meeting**: August 5, 2025, 10:00 AM (Virtual).
- **Additional Notes**:
    - Jane Smith emphasized the need for proactive communication on changes.
    - CloudSafe agreed to provide a monthly summary report starting June 2025 to streamline reviews.

Prepared by: Jane Smith, IT Manager, Tech Solutions
Approved by: John Doe, Information Security Officer, Tech Solutions
Date Prepared: May 5, 2025

1.3 Information security for use of cloud services (5.23)

Control 5.23:

Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.

Control attributes:

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

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventive	Confidentiality Integrity (Availability	Protect	Supplier_relation-ships_security	#Governance_and_ Ecosystem #Protec-tion

Control description:

- Your organization needs a clear policy about how to use cloud services securely (Example: Imagine your company uses Dropbox for file storage. The policy might say, "Only approved employees can store work files in Dropbox, and sensitive data like customer info must be encrypted." You share this policy through email or a company handbook so everyone understands the rules.)
- You need to explain how your organization will identify and handle risks when using cloud services (Example: Suppose you use Amazon Web Services (AWS) for hosting your app. A risk might be that AWS servers could go down, affecting your app. Your plan might include checking AWS's security features and having a backup server elsewhere)
- Cloud services involve teamwork. The cloud provider (e.g., Microsoft) handles some security tasks, and your organization handles others. You need to clearly define who does what (Example: If you use Microsoft Azure, Microsoft might secure the physical

servers (their responsibility), but you need to set strong passwords and manage user access (your responsibility))

- List what security measures are needed for the cloud service (Example: For Google Cloud, you might require that all data is encrypted and only accessible by specific team members)
- Decide which cloud services to use and what they'll be used for (Example: You choose Google Drive for file sharing but not for storing sensitive financial data. You document why Google Drive was picked (e.g., it's cost-effective and secure))
- Clarify who in your company manages the cloud service (Example: Your IT manager approves new users for AWS)
- Specify which security tasks the provider handles and which you handle (Example: For Dropbox, Dropbox manages server security, but you manage who can view or edit files)
- Learn and use the security tools the cloud provider offers (Example: AWS offers two-factor authentication (2FA). You ensure all employees enable 2FA for their AWS accounts)
- Verify that the cloud provider's security measures are working (Example: You ask Microsoft Azure for a report showing they meet security standards like ISO 27001)
- If you use multiple providers, ensure they work together smoothly and securely (Example: You use AWS for hosting and Google Cloud for analytics. You set up secure data transfers between them and monitor both for issues)
- Have a plan for dealing with security problems, like data breaches (Example: If a hacker accesses your Google Drive, your plan might include notifying Google, locking affected accounts, and informing customers if needed)
- Regularly check if the cloud service is still secure and meets your needs (Example: Every six months, you review AWS logs to ensure no unauthorized access and check if AWS still fits your budget and security needs)
- Plan how to switch providers or stop using a cloud service without losing data (Example: If you stop using Dropbox, your plan might include downloading all files, transferring them to another service, and securely deleting data from Dropbox)
- Cloud providers often have standard contracts that you can't change. You need to read these agreements to ensure they meet your security needs (e.g., keeping data confidential, available, and intact). You should also assess risks to spot any gaps (Example: You're considering Salesforce for customer data. You read their agreement to confirm they encrypt data and guarantee 99.9% uptime)

Control evidence:

Checks to be performed	Evidence
➢ Whether a specific policy on the use of cloud services is established and communicated to all interested parties ➢ Whether a process for managing information security risks associated with the use of cloud services is defined and communicated ➢ Whether the responsibilities of the cloud service provider and the organization, as a customer of the cloud services, are defined and implemented appropriately ➢ Whether all information security requirements associated with the use of cloud services are defined ➢ Whether the functions and responsibilities relating to the use and management of cloud services are defined ➢ Whether the way to change or stop the use of cloud services, including exit strategies from cloud services is defined ➢ If a contract with the cloud service provider guaranteeing the protection of the organization's data and ensuring the availability of services is signed	➢ Specific policy for the use of cloud services ➢ Information security risk management document associated with the use of cloud services ➢ List of functions and responsibilities related to the use and management of cloud services ➢ Information Security Incident Management Procedure ➢ Contracts and guarantees signed with cloud service providers

TECH SOLUTIONS

Tech Solutions Cloud Services Security Policy

Purpose

This policy ensures that **Tech Solutions** securely uses cloud services to protect the confidentiality, integrity, and availability of information, in compliance with **ISO 27001:2022 Clause 5.23**. It establishes rules for selecting, managing, and monitoring cloud services and defines responsibilities for both Tech Solutions and cloud service providers. This policy applies to all employees, contractors, and third parties using cloud services on behalf of Tech Solutions.

Scope

This policy covers all cloud services used by Tech Solutions, including:

- **Amazon Web Services (AWS)** for application hosting and storage.
- **Google Workspace** for email and document collaboration.
- **Microsoft Azure** for data analytics and machine learning.

Policy Statements

1. Cloud Service Selection and Approval

- **Requirement**: Cloud services must be selected based on defined criteria and approved before use.
- **Details**:
  - Selection criteria include compliance with ISO 27001, encryption capabilities, uptime guarantees (minimum 99.9%), and cost-effectiveness.
  - The Information Security Officer (ISO) must approve all cloud services.
  - Scope of usage (e.g., type of data or processes) is documented for each service.
- **Example**: AWS is selected for hosting client applications because it offers ISO 27001 certification and encryption. Its use is limited to non-sensitive application data, as approved by the ISO.

2. Information Security Requirements

- **Requirement**: Cloud services must meet specific information security requirements.
- **Details**:

    - Data must be encrypted at rest (e.g., AES-256) and in transit (e.g., TLS 1.2 or higher).
    - Access controls must include role-based access and two-factor authentication (2FA).
    - Sensitive data (e.g., client personal data) requires additional controls, such as restricted sharing.
- **Example**: Google Workspace is configured to encrypt emails and documents, with 2FA enabled for all users and sensitive client folders accessible only to project managers.

3. Roles and Responsibilities

- **Requirement**: Roles and responsibilities for cloud service management are defined.
- **Details**:
    - **Information Security Officer (ISO)**: Approves cloud services, reviews agreements, and oversees compliance.
    - **IT Team**: Configures security settings, monitors usage, and responds to incidents.
    - **Employees**: Use cloud services per this policy and report security issues.
    - **Cloud Service Providers**: Maintain infrastructure security and provide compliance reports.
- **Example**: The ISO approves Microsoft Azure for analytics, the IT team sets up user permissions, and employees report suspicious login attempts.

4. Shared Responsibilities

- **Requirement**: Responsibilities between Tech Solutions and cloud service providers are clearly defined and implemented.
- **Details**:
    - **Provider Responsibilities**: Physical security, network security, and platform-level patches.
    - **Tech Solutions Responsibilities**: User account management, access control configuration, and data classification.
    - A responsibility matrix is maintained for each cloud service.
- **Example**: AWS secures its data centers and applies server patches, while Tech Solutions configures AWS Identity and Access Management (IAM) to limit developer access to production data.

5. Utilizing Provider Security Capabilities

- **Requirement**: Tech Solutions will leverage security features provided by cloud services.
- **Details**:
    - Enable provider tools like encryption, logging, and intrusion detection.
    - Provide training to employees on using these tools.
- **Example**: AWS CloudTrail is enabled to log all account activity, and the IT team is trained to review logs for unauthorized access attempts.

6. Assurance of Provider Controls

- **Requirement**: Verify that cloud providers implement effective security controls.
- **Details**:
  - Request and review provider certifications (e.g., ISO 27001, SOC 2) annually.
  - Obtain third-party audit reports or attestations.
  - Conduct risk assessments to identify gaps in provider controls.
- **Example**: The ISO reviews Google Workspace's SOC 2 report annually and confirms encryption standards meet client requirements.

7. Managing Multiple Cloud Services

- **Requirement**: Ensure secure integration and management of multiple cloud services.
- **Details**:
  - Use secure APIs and encrypted connections (e.g., HTTPS) for data transfers between services.
  - Maintain an inventory of all cloud services, updated quarterly.
  - Monitor interfaces for compatibility and security issues.
- **Example**: Data is transferred from AWS to Azure for analytics via a secure API. The IT team tracks both services in a cloud inventory spreadsheet.

8. Incident Handling Procedures

- **Requirement**: Procedures are established for handling information security incidents in cloud services.
- **Details**:
  - Incidents (e.g., unauthorized access) must be reported to the IT team within 1 hour.
  - Collaborate with the provider to investigate and mitigate incidents.
  - Document incidents and notify affected parties per legal or contractual obligations.
- **Example**: If a Google Workspace account is compromised, the IT team locks the account, resets credentials, contacts Google for breach details, and logs the incident for review.

9. Monitoring, Reviewing, and Evaluating Cloud Services

- **Requirement**: Continuously monitor and periodically review cloud services to manage security risks.
- **Details**:
  - Monitor usage logs and security alerts in real-time.
  - Conduct quarterly reviews of service performance, security controls, and compliance.
  - Update risk assessments annually or after significant changes.
- **Example**: The IT team uses AWS CloudWatch to monitor server activity and reviews Azure security settings every three months to ensure compliance.

10. Changing or Terminating Cloud Services

- **Requirement**: Define an exit strategy for changing or stopping cloud services.
- **Details**:
  - Back up all data before termination.
  - Transfer data to a new provider using encrypted channels.
  - Verify data deletion from the old provider via a deletion certificate.
  - Update risk assessments after changes.
- **Example**: To stop using Google Workspace, the IT team downloads all files, migrates them to Microsoft 365, requests a deletion certificate from Google, and updates the risk register.

11. Cloud Service Agreements

- **Requirement**: Review cloud service agreements to ensure they meet security needs.
- **Details**:
  - Agreements must address confidentiality (e.g., non-disclosure), integrity (e.g., data accuracy), and availability (e.g., uptime guarantees).
  - Include service level objectives (SLOs) like 99.9% uptime and qualitative objectives like timely incident response.
  - Conduct risk assessments to identify gaps and implement compensating controls (e.g., additional backups).
- **Example**: The AWS agreement specifies 99.9% uptime and data encryption. A risk assessment identifies the need for daily offsite backups to mitigate data loss risks, which Tech Solutions implements.

Risk Management Approach

- **Integration with Existing Processes**: Cloud service risks are managed as part of Tech Solutions' broader third-party risk management process (aligned with ISO 27001 Clauses 5.21 and 5.22).
- **Process**:
  - Identify risks (e.g., provider downtime, data breaches) during service selection and annually.
  - Assess risks using a likelihood-impact matrix.
  - Mitigate risks through controls (e.g., encryption, backups) or contractual terms.
  - Document risks in the risk register and review quarterly.
- **Example**: A risk assessment for Azure identifies a potential data breach risk. Tech Solutions mitigates this by enabling 2FA and restricting data access to authorized users.

Communication

- This policy is communicated to all employees and relevant parties (e.g., contractors) via:
  - Email distribution upon policy approval or updates.
  - Company intranet under the "Information Security" section.
  - Mandatory training during employee onboarding and annual refreshers.

- Clients are informed of our cloud security practices upon request to ensure transparency.

Compliance and Enforcement

- Compliance with this policy is mandatory. Violations may result in disciplinary action, up to termination.
- The ISO conducts annual audits to verify adherence.
- Non-compliance by cloud providers triggers a review and potential termination of the service.

Contact

For questions, incident reports, or clarification, contact the Information Security Officer at security@techsolutions.com.

Review

This policy is reviewed annually or after significant changes to cloud services or ISO 27001 requirements. Last updated: **May 5, 2025**.

TECH SOLUTIONS

Tech Solutions Information Security Risk Management Document for Cloud Services

Purpose

This document outlines how **Tech Solutions** manages information security risks associated with the use of cloud services, in compliance with ISO 27001 clause 5.23. It ensures that risks to data confidentiality, integrity, and availability are identified, assessed, and mitigated when using cloud services such as **Amazon Web Services (AWS)**, **Google Workspace**, and **Microsoft Azure**.

Scope

This document applies to all cloud services used by Tech Solutions for storing, processing, or transmitting company or client data. It builds on our existing risk management framework for external services (aligned with ISO 27001 clauses 5.21 and 5.22).

1. Risk Management Approach

Tech Solutions uses a systematic process to manage cloud service risks, integrated with our broader information security management system (ISMS). The process includes:

- **Identification**: Listing potential risks specific to cloud services.
- **Assessment**: Evaluating the likelihood and impact of each risk.
- **Treatment**: Implementing controls to reduce risks to an acceptable level.
- **Monitoring**: Regularly reviewing risks and controls.

2. Roles and Responsibilities

- **IT Manager**: Oversees risk assessments, approves risk treatment plans, and ensures compliance with this document.
- **Security Team**: Conducts risk assessments and implements controls.
- **Employees**: Report potential risks or incidents to the Security Team.
- **Cloud Service Providers**: Provide security features and reports as per agreements.

Example: The IT Manager approves the use of AWS, while the Security Team configures access controls and monitors logs.

3. Risk Identification

The following risks are commonly associated with cloud services used by Tech Solutions:

Risk ID	Risk Description	Example Scenario
R1	Unauthorized access to cloud data	A hacker guesses an employee's Google Workspace password, accessing client contracts.
R2	Data loss due to provider outage	AWS experiences a server outage, making client applications unavailable.
R3	Misconfiguration of cloud settings	An employee accidentally makes an Azure database publicly accessible.
R4	Data breach by cloud provider	A vulnerability in Google Workspace exposes stored documents.
R5	Non-compliance with regulations	AWS fails to meet GDPR requirements for client data, risking fines.
R6	Insecure data transfer between clouds	Data sent from AWS to Azure is intercepted due to unencrypted connections.
R7	Vendor lock-in	Difficulty migrating data from Google Workspace to another provider, causing delays.

4. Risk Assessment

Each risk is assessed based on **likelihood** (how likely it is to occur) and **impact** (how severe the consequences would be). We use a simple 3x3 risk matrix:

Likelihood	Impact	Risk Level
Low (1)	Low (1)	Low (1-2)
Medium (2)	Medium (2)	Medium (3-4)
High (3)	High (3)	High (6-9)

Risk Assessment Example:

- **Risk R1 (Unauthorized access)**:
  - **Likelihood**: Medium (2) – Weak passwords are common without 2FA.
  - **Impact**: High (3) – Client data exposure could harm reputation and lead to legal issues.
  - **Risk Level**: 2 x 3 = 6 (High).

5. Risk Treatment Plan

For each identified risk, Tech Solutions implements controls to reduce the risk to an acceptable level. Controls are divided between those managed by Tech Solutions and those managed by the cloud service provider.

Risk ID	Control Description	Responsibility	Example Implementation
R1	Enable two-factor authentication (2FA)	Tech Solutions	Require 2FA for all Google Workspace accounts.
R1	Regular password audits	Tech Solutions	Check for weak passwords quarterly using a password manager tool.
R2	Implement data backups	Tech Solutions	Back up AWS data to a secondary provider (e.g., Google Cloud) daily.
R2	Service availability monitoring	Cloud Provider	AWS provides 99.9% uptime as per the service agreement.
R3	Restrict configuration changes	Tech Solutions	Limit Azure configuration changes to the Security Team.
R3	Regular security audits	Tech Solutions	Conduct monthly checks of Azure settings using a checklist.
R4	Review provider security certifications	Tech Solutions	Verify Google Workspace's ISO 27001 certification annually.
R4	Encrypt sensitive data	Tech Solutions	Use client-side encryption for sensitive files in Google Workspace.
R5	Verify provider compliance	Tech Solutions	Request AWS GDPR compliance reports before storing client data.
R6	Use encrypted data transfers	Tech Solutions	Configure AWS-to-Azure transfers using HTTPS and secure APIs.
R7	Develop an exit strategy	Tech Solutions	Document a process to export Google Workspace data and delete accounts.

Example: For R1, Tech Solutions enforces 2FA on Google Workspace, reducing the likelihood of unauthorized access from Medium (2) to Low (1), lowering the risk level to 1 x 3 = 3 (Medium).

6. Shared Responsibilities

Tech Solutions and cloud providers share security responsibilities:

- **Cloud Provider Responsibilities**:
  - Secure physical infrastructure (e.g., AWS data centers).
  - Maintain platform security (e.g., Google Workspace patches).
  - Provide security tools (e.g., Azure's role-based access control).
- **Tech Solutions Responsibilities**:
  - Configure access controls and user permissions.

    - Monitor account activity and logs.
    - Train employees on secure cloud usage.

Example: Microsoft Azure secures its servers, but Tech Solutions configures user roles to ensure only authorized analysts access client data.

7. Utilizing Provider Capabilities

Tech Solutions leverages security features offered by cloud providers:

- **AWS**: Enable CloudTrail for activity logging and Security Hub for compliance checks.
- **Google Workspace**: Use Data Loss Prevention (DLP) to prevent sensitive data leaks.
- **Azure**: Implement Key Vault for secure storage of encryption keys.

Example: The Security Team enables AWS CloudTrail and reviews logs monthly to detect unauthorized access attempts.

8. Assurance of Provider Controls

To ensure providers meet security standards:

- Request and review certifications (e.g., ISO 27001, SOC 2).
- Analyze provider audit reports annually.
- Conduct risk assessments before renewing contracts.

Example: The IT Manager reviews AWS's SOC 2 report to confirm compliance with data security requirements.

9. Managing Multiple Cloud Services

When using multiple providers (e.g., AWS and Azure):

- Use secure, encrypted connections for data transfers.
- Maintain a central inventory of cloud services and their configurations.
- Monitor interfaces for compatibility issues.

Example: Data transferred from AWS to Azure for analytics is encrypted using TLS, and the IT team tracks both services in a shared dashboard.

10. Incident Handling

Procedures for cloud-related security incidents:

- **Detection**: Monitor logs and alerts (e.g., AWS CloudWatch).
- **Response**: Isolate affected systems, reset credentials, and contact the provider.
- **Reporting**: Notify the IT Manager and, if necessary, clients within 24 hours.
- **Recovery**: Restore data from backups and update controls.

Example: If a Google Workspace breach is detected, the Security Team locks the affected account, works with Google to investigate, and restores files from backups.

11. Monitoring and Review

- **Frequency**: Conduct risk assessments quarterly or after significant changes (e.g., new cloud service adoption).
- **Methods**: Review logs, audit configurations, and evaluate provider performance.
- **Updates**: Adjust risk treatments if new risks emerge or existing controls fail.

Example: Every three months, the Security Team reviews Azure access logs and updates user permissions if employees change roles.

12. Exit Strategies

To change or terminate cloud services:

- Back up all data to a secure location.
- Transfer data to a new provider using encrypted channels.
- Verify data integrity after transfer.
- Delete data from the old provider and confirm deletion.

Example: To stop using Google Workspace, the IT team exports all files to Microsoft 365, verifies the transfer, and then deletes the Google Workspace account.

13. Cloud Service Agreements

Tech Solutions reviews cloud service agreements to ensure they address:

- **Confidentiality**: Data is protected from unauthorized access.
- **Integrity**: Data remains accurate and unaltered.
- **Availability**: Services meet uptime guarantees (e.g., 99.9%).
- **Risk Gaps**: Additional controls (e.g., backups) are implemented if agreements lack coverage.

Example: The AWS agreement ensures 99.9% uptime but doesn't cover user error data loss. Tech Solutions adds daily backups to Google Cloud to mitigate this risk.

Communication

- This document is shared with all employees via the company intranet and email.
- Training sessions are held annually to explain the risk management process.
- Updates are communicated through team meetings and email alerts.

Compliance

- The IT Manager audits compliance with this document annually.
- Non-compliance (e.g., using unapproved cloud services) may result in disciplinary action.

Contact

For questions or to report risks/incidents, contact the IT Manager at it.manager@techsolutions.com.

TECH SOLUTIONS

Tech Solutions Cloud Services Incident Management Procedure

Purpose

This procedure outlines how **Tech Solutions**, a software development and IT consulting company, manages information security incidents related to cloud services (e.g., Amazon Web Services, Google Workspace, Microsoft Azure) to ensure compliance with ISO 27001 clause 5.23. It ensures timely detection, response, and recovery from incidents while clarifying responsibilities shared with cloud service providers.

Scope

This procedure applies to all cloud services used by Tech Solutions and covers incidents such as:

- Unauthorized access to cloud accounts.
- Data breaches or leaks in cloud storage.
- Service disruptions caused by security issues (e.g., ransomware).
- Misconfiguration of cloud security settings.

Definitions

- **Incident**: Any event that compromises the confidentiality, integrity, or availability of data in a cloud service (e.g., a hacked Google Workspace account).
- **Cloud Service Provider (CSP)**: The company providing the cloud service (e.g., AWS, Google, Microsoft).
- **Incident Manager**: The designated Tech Solutions employee responsible for coordinating incident response (typically the IT Manager).

Procedure

1. Incident Identification

- **Objective**: Detect potential security incidents in cloud services quickly.
- **Steps**:
    - Employees monitor cloud service dashboards and logs for unusual activity (e.g., AWS CloudTrail alerts for multiple failed login attempts).

    - Cloud providers' automated notifications (e.g., Google Workspace security alerts) are configured to notify the IT team.
    - Employees report suspected incidents (e.g., unexpected file deletions in Microsoft Azure) to the Incident Manager via email (it.manager@techsolutions.com) or phone within 1 hour.
- **Example**: An employee notices a client's data folder in Google Workspace is accessible to an unknown user. They report it immediately.

2. Incident Reporting

- **Objective**: Ensure incidents are formally documented and communicated.
- **Steps**:
    - The reporting employee provides details: date, time, cloud service involved, and a description of the issue.
    - The Incident Manager logs the incident in the **Incident Register** (a secure spreadsheet stored in Google Workspace with restricted access).
    - The Incident Manager notifies the cloud provider's support team if the incident involves their infrastructure (e.g., contacting AWS support for a suspected server breach).
- **Example**: The Incident Manager logs an unauthorized AWS login attempt and emails AWS support with the incident details, including the affected account ID.

3. Incident Assessment

- **Objective**: Evaluate the incident's severity and impact.
- **Steps**:
    - The Incident Manager determines the incident's scope (e.g., which data or systems are affected) and severity (low, medium, high).
        - **Low**: Minor misconfiguration with no data exposure (e.g., public access to an empty AWS S3 bucket).
        - **Medium**: Limited data exposure or service disruption (e.g., a shared Google Workspace document accessed by an unauthorized user).
        - **High**: Major data breach or service outage (e.g., client data stolen from Microsoft Azure).
    - The Incident Manager collaborates with the cloud provider to confirm their role in the incident (e.g., was it a provider-side failure or a Tech Solutions configuration error?).
- **Example**: A medium-severity incident is identified when a Google Workspace folder containing non-sensitive client proposals is shared publicly due to a user error.

4. Incident Containment

- **Objective**: Limit the incident's impact and prevent further damage.
- **Steps**:
    - **Tech Solutions Actions**:
        - Suspend affected user accounts or revoke access (e.g., disable a compromised AWS user account).
        - Adjust security settings (e.g., enable 2FA on a Google Workspace account).

        - Isolate affected systems (e.g., temporarily disable a misconfigured Azure virtual machine).
    - **Cloud Provider Actions**:
        - The Incident Manager requests the provider to take actions like locking accounts or restoring data, as per the shared responsibility model.
    - Document all containment actions in the Incident Register.
- **Example**: For a compromised Google Workspace account, the Incident Manager resets the user's password, enables 2FA, and asks Google to verify if other accounts were affected.

5. Incident Eradication

- **Objective**: Remove the cause of the incident and secure the cloud service.
- **Steps**:
    - Address the root cause (e.g., fix a misconfigured AWS S3 bucket setting that allowed public access).
    - Apply patches or updates provided by the cloud provider (e.g., update Azure security configurations).
    - The Incident Manager verifies with the cloud provider that their systems are secure (e.g., AWS confirms no further unauthorized access).
- **Example**: A public Google Workspace folder is made private, and the IT team checks all other folders to ensure correct permissions.

6. Incident Recovery

- **Objective**: Restore normal operations and verify security.
- **Steps**:
    - Restore affected data or services from backups (e.g., recover deleted files from Google Workspace's backup).
    - Test the cloud service to ensure it's functioning securely (e.g., confirm AWS application access is restored).
    - Notify employees when the service is safe to use again.
- **Example**: After resolving a data deletion incident in Microsoft Azure, the IT team restores the data from a backup and tests the analytics dashboard to confirm it works.

7. Incident Notification

- **Objective**: Inform relevant parties as required.
- **Steps**:
    - If client data is affected, the Incident Manager notifies clients within 72 hours, as per contractual or legal obligations (e.g., GDPR).
    - Report high-severity incidents to regulatory authorities if required.
    - Communicate with the cloud provider to confirm their notification responsibilities (e.g., AWS may notify their users if their infrastructure was compromised).
- **Example**: A breach in AWS exposes client data. The Incident Manager emails affected clients with details and mitigation steps, while AWS notifies their broader user base if needed.

8. Post-Incident Review

- **Objective**: Learn from the incident to prevent recurrence.
- **Steps**:
  - Within 7 days, the Incident Manager holds a review meeting with the IT team and, if necessary, the cloud provider.
  - Document lessons learned (e.g., "AWS S3 buckets need regular permission audits").
  - Update security controls, policies, or training based on findings (e.g., add a mandatory 2FA training session).
  - Update the Incident Register with the review outcomes.
- **Example**: After a Google Workspace incident, the team realizes employees need better training on sharing settings. A training session is scheduled, and the Cloud Services Policy is updated.

9. Documentation and Record-Keeping

- **Objective**: Maintain records for compliance and audits.
- **Steps**:
  - All incident details, actions, and outcomes are recorded in the Incident Register.
  - Records are retained for at least 3 years, stored securely in Google Workspace with restricted access.
  - The Incident Manager provides incident reports to auditors during ISO 27001 reviews.
- **Example**: The Incident Register includes details of an Azure incident, including timestamps, actions taken, and the final resolution.

Roles and Responsibilities

- **Incident Manager (IT Manager)**:
  - Coordinates the incident response process.
  - Communicates with the cloud provider and internal teams.
  - Updates the Incident Register and leads post-incident reviews.
- **Employees**:
  - Report suspected incidents promptly.
  - Follow containment and recovery instructions.
- **Cloud Service Provider**:
  - Provides support for incidents involving their infrastructure.
  - Shares relevant logs, reports, or recovery tools as per the service agreement.

Communication

- Employees are trained on this procedure during onboarding and annually.
- The procedure is available on the company intranet and emailed to all staff.
- During an incident, the Incident Manager uses email and phone to communicate updates to relevant teams.

Monitoring and Compliance

- The IT Manager conducts quarterly reviews of the Incident Register to identify trends (e.g., repeated AWS misconfigurations).
- Non-compliance with this procedure (e.g., failing to report an incident) may result in disciplinary action.
- The procedure is audited annually as part of ISO 27001 compliance.

Contact

For incident reporting or questions, contact the Incident Manager at it.manager@techsolutions.com or (555) 123-4567.

1.5 Information security incident management planning and preparation (5.24)

Control 5.24:

The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

Control attributes:

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

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Corrective	Confidentiality Integrity Availability	Protect	Respond, Recover	Governance Information_security_event_management

Control description:

- Your organization needs a clear plan to deal with security incidents (e.g., a hacker accessing your system or an employee losing a laptop with sensitive data). This plan should outline how to detect, respond to, and recover from these incidents.

  Example: Imagine you run a small online store. If your website gets hacked and customer data is stolen, you need a process to:

  Detect the hack (e.g., unusual activity in your system).

  Respond (e.g., block the hacker's access).

  Recover (e.g., restore the website and notify customers).

- Decide who in your organization is responsible for handling security incidents and make sure everyone (including external partners like IT vendors) knows their role.

Example: In your online store:

The IT manager might be responsible for fixing the hack.

The customer service team could handle notifying affected customers.

An external cybersecurity firm might help investigate the breach. You'd write down these roles and share them with everyone involved

- Set up an easy way for employees or others to report security issues, including a clear point of contact.

  Example: In your store, you could create an email address like security@yourstore.com or a form on your internal website where employees can report issues (e.g., "I clicked a suspicious link in an email"). The IT manager is the point of contact to handle these reports.

- Create a process to manage incidents from start to finish, including:

  Recording the incident (administration and documentation).

  Detecting and analyzing the issue (detection, triage, analysis).

  Deciding how serious it is (prioritization).

  Communicating with the right people (communication).

  Coordinating with everyone involved (coordination).

  Example: If an employee reports a phishing email:

  Record: Log the incident in a tracking system.

  Detect/Analyze: Check if the email installed malware.

  Prioritize: If it's a serious threat (e.g., malware spreading), act immediately.

  Communicate: Inform the IT team and management.

  Coordinate: Work with an external IT vendor to remove the malware.

- Build a process to assess incidents, respond to them, and learn from them to prevent future issues.

Example: After the phishing email incident:

Assess: Determine how the email got through your spam filter.

Respond: Remove the malware and reset affected passwords.

Learn: Train employees on spotting phishing emails and update your email filters.

- Only trained and qualified people should handle security incidents. They need clear instructions (procedure documentation) and regular training.

  Example: Your IT manager should be trained in cybersecurity basics. You give them a written guide on handling incidents (e.g., “Step 1: Isolate the affected computer”). Every six months, they attend a short training session on new cyber threats.

- Set up a process to identify what training or certifications your incident response team needs and ensure they keep learning.

  Example: Your IT manager might need a basic cybersecurity certification like CompTIA Security+. You create a plan to:

  Send them to a training course.

  Schedule annual refreshers on new threats.

  Encourage them to read cybersecurity blogs to stay updated

- Management should ensure there’s a detailed plan for handling incidents, covering various scenarios and procedures for key activities (e.g., detecting, responding, recovering).

  Example: Your store’s incident management plan might include:

  A list of possible incidents (e.g., hacking, data leaks, ransomware).

  Procedures for each, like:

  Detection: Use antivirus software to spot threats.

  Response: Follow a checklist to contain the issue (e.g., disconnect affected systems).

  Recovery: Restore systems from backups and inform customers if needed.

Control evidence:

Checks to be performed	Evidence
➢ if an Incident Management Procedure exists ➢ Whether responsibilities for ensuring effective incident management are defined and documented ➢ Whether a schema exists that includes criteria for categorizing events as information security incidents ➢ Whether the point of contact assesses each information security event using the schema ➢ Whether the personnel responsible for responding to information security incidents make a decision on information security events ➢ Whether the results of the event assessment and the decisions taken are recorded in detail	➢ Incident Management Procedure ➢ Document defining responsibilities relating to incident management ➢ Job descriptions of personnel assigned to incident management ➢ Records of security event processing results

TECH SOLUTIONS

Information Security Incident Management Procedure

1. Purpose

This procedure outlines how **Tech Solutions** manages information security incidents (e.g., data breaches, malware infections, unauthorized access) to protect our systems, data, and customers. It ensures incidents are detected, reported, responded to, and resolved efficiently, in line with ISO 27001 requirements.

2. Scope

This procedure applies to all employees, contractors, and third-party vendors working with Tech Solutions' information systems, including servers, cloud platforms, employee devices, and customer data.

3. Definitions

- **Information Security Incident**: Any event that compromises the confidentiality, integrity, or availability of information (e.g., a hacker accessing customer data or a lost laptop with sensitive files).
- **Incident Response Team (IRT)**: A group responsible for managing security incidents.

4. Roles and Responsibilities

The following roles are assigned to ensure effective incident management:

Role	Responsibilities
Information Security Manager	Oversees the incident management process, coordinates the IRT, and reports to management.
IT Team	Detects, analyzes, and contains incidents (e.g., isolates affected systems).
Human Resources (HR)	Handles incidents involving employee misconduct and communicates with staff.
Customer Support Team	Notifies customers affected by incidents and manages external communications.
External Cybersecurity Vendor	Provides expert support for complex incidents (e.g., ransomware recovery).
All Employees	Report suspected security incidents immediately to the designated point of contact.

These roles are communicated to all staff via the company intranet and during onboarding. External vendors receive a summary of their responsibilities in their contracts.

5. Incident Management Objectives

Tech Solutions' management has agreed on the following objectives:

- Resolve critical incidents (e.g., data breaches) within **24 hours**.
- Minimize disruption to business operations and customer services.
- Learn from incidents to prevent recurrence.
- Comply with legal and contractual obligations (e.g., notifying customers of breaches).

6. Incident Management Process

The process for managing information security incidents includes the following steps:

6.1. Reporting Incidents

- **How to Report**: Employees, contractors, or vendors must report suspected incidents (e.g., phishing emails, unusual system behavior) immediately via:
  - Email: security@techsolutions.com
  - Phone: +1-800-SEC-1234 (available 24/7)
  - Internal web form on the company intranet (under "Report a Security Issue").
- **Point of Contact**: The Information Security Manager is the primary contact for all reports.
- **Example**: An employee receives a suspicious email with a link. They forward it to security@techsolutions.com and avoid clicking the link.

6.2. Incident Management Workflow

The Incident Response Team (IRT) follows these steps for each reported incident:

1. **Administration and Documentation**:
    - Log the incident in the **Incident Tracking System** (a secure internal database).
    - Record details like date, time, reporter, and initial description.
    - Example: A reported phishing email is logged with the email's subject and sender.
2. **Detection and Triage**:
    - Confirm the incident (e.g., verify if the email contains malware).
    - Assess the scope (e.g., did it affect one user or multiple systems?).
    - Example: The IT Team scans the employee's computer for malware.
3. **Prioritization**:
    - Assign a severity level based on impact and urgency:
        - **Critical**: Affects customer data or core systems (e.g., a server breach).
        - **High**: Disrupts operations but no data loss (e.g., DDoS attack).
        - **Medium**: Limited impact (e.g., a single compromised account).
        - **Low**: No immediate impact (e.g., a failed login attempt).
    - Example: A ransomware attack encrypting customer data is marked "Critical."
4. **Analysis**:
    - Investigate the root cause (e.g., how the ransomware entered the system).
    - Identify affected systems, data, or users.
    - Example: The IT Team finds the ransomware came from a phishing email.
5. **Communication**:
    - Notify the IRT and management about the incident's status.
    - Inform affected customers or authorities if required (e.g., data breach notifications).
    - Example: The Customer Support Team emails affected customers about the breach.
6. **Coordination**:
    - Work with internal teams and external vendors to resolve the incident.
    - Example: The external cybersecurity vendor helps decrypt files affected by ransomware.

6.3. Incident Response Process

The IRT follows these steps to respond to incidents:

1. **Assessment**:
    - Evaluate the incident's impact (e.g., how much data was compromised?).
    - Example: Check if customer payment details were stolen during a breach.
2. **Containment**:
    - Take immediate actions to limit damage (e.g., isolate affected servers, reset passwords).
    - Example: Disconnect a hacked server from the network.
3. **Eradication**:
    - Remove the threat (e.g., delete malware, patch vulnerabilities).
    - Example: Update software to fix the vulnerability exploited by the ransomware.

4. **Recovery**:
    - Restore systems and data (e.g., use backups to recover encrypted files).
    - Verify systems are secure before resuming operations.
    - Example: Restore the server from a backup and test it for malware.
5. **Lessons Learned**:
    - Conduct a post-incident review to identify improvements.
    - Update policies, training, or systems to prevent recurrence.
    - Example: Train employees on spotting phishing emails after a ransomware incident.

6.4. Competent Personnel

- Only trained personnel handle incidents. The IRT includes:
    - **Information Security Manager**: Holds a CompTIA Security+ certification.
    - **IT Team Members**: Trained in basic cybersecurity and incident response.
    - **External Vendor**: A certified cybersecurity firm with expertise in incident recovery.
- All IRT members receive:
    - A detailed **Incident Response Handbook** (available on the intranet).
    - Annual training on new threats and response techniques.
    - Example: The IT Team attends a workshop on ransomware defense.

6.5. Training and Certification

- **Training Needs**:
    - New IRT members complete an introductory cybersecurity course within 3 months.
    - Annual refresher training on incident response (e.g., simulations of phishing attacks).
- **Certifications**:
    - Information Security Manager: Maintains CompTIA Security+ or equivalent.
    - IT Team: Encouraged to pursue certifications like Certified Ethical Hacker (CEH).
- **Ongoing Development**:
    - IRT members subscribe to cybersecurity newsletters (e.g., Krebs on Security).
    - Attend at least one industry webinar or conference per year.
- Example: The Information Security Manager attends a webinar on cloud security trends.

7. Incident Management Scenarios

The following scenarios outline specific procedures for common incidents at Tech Solutions:

Scenario 1: Phishing Email

- **Detection**: An employee reports a suspicious email to security@techsolutions.com.
- **Response**:
  - IT Team scans the email and employee's device for malware.
  - Block the sender's email address in the company's email system.
- **Recovery**: Reset the employee's password if compromised.
- **Lessons Learned**: Conduct a company-wide phishing awareness session.

Scenario 2: Data Breach on Cloud Platform

- **Detection**: Intrusion detection software flags unauthorized access to a cloud server.
- **Response**:
  - Isolate the server by revoking access credentials.
  - Engage the external cybersecurity vendor to analyze the breach.
- **Recovery**:
  - Restore data from backups.
  - Notify affected customers within 24 hours, as per legal requirements.
- **Lessons Learned**: Implement multi-factor authentication (MFA) for all cloud accounts.

Scenario 3: Lost Employee Laptop

- **Detection**: An employee reports a lost laptop to HR or the Information Security Manager.
- **Response**:
  - Remotely wipe the laptop using mobile device management (MDM) software.
  - Disable the employee's account to prevent unauthorized access.
- **Recovery**: Provide a replacement laptop with updated security settings.
- **Lessons Learned**: Review laptop encryption policies to ensure all devices are secure.

8. Incident Management Plan

The **Information Security Incident Management Plan** includes:

- A list of potential incidents (e.g., phishing, data breaches, ransomware, lost devices).
- Procedures for each scenario (as above).
- Tools used:
  - **Intrusion Detection System**: Monitors network traffic for threats.
  - **Incident Tracking System**: Logs and tracks incidents.
  - **Backup Software**: Ensures data can be restored after incidents.
- Regular testing:
  - Conduct quarterly incident response drills (e.g., simulate a data breach).
  - Update the plan annually or after major incidents.

9. Management Oversight

- **Approval**: The CEO and Information Security Manager review and approve this procedure annually.
- **Priorities**: Management ensures incidents affecting customer data or core services are resolved within 24 hours.
- **Reporting**: The Information Security Manager provides a monthly incident report to management, summarizing incidents and lessons learned.

10. Review and Improvement

- This procedure is reviewed annually or after significant incidents.
- Feedback from the IRT and employees is incorporated to improve the process.
- Example: After a phishing incident, employees suggested simplifying the reporting form, which was updated.

11. Contact Information

For questions or to report an incident:

- **Email**: security@techsolutions.com
- **Phone**: +1-800-SEC-1234
- **Intranet**: Access the Incident Response Handbook and reporting form at intranet.techsolutions.com/security.

Document Version: 1.0
Approved By: Jane Doe, CEO
Date: May 5, 2025

Incident Management Responsibilities Document

Date: May 05, 2025
Version: 1.0
Prepared by: Information Security Team
Approved by: Chief Information Security Officer (CISO)

---

1. Purpose

This document defines the roles and responsibilities for managing information security incidents at Tech Solutions. It ensures compliance with ISO 27001 requirements and supports our commitment to protecting customer data, company assets, and business operations.

Objectives

- Respond to security incidents quickly and effectively.
- Minimize the impact of incidents on operations and customers.
- Learn from incidents to improve security.
- Ensure clear communication with internal and external parties.

---

2. Scope

This document applies to all employees, contractors, and third-party vendors working with Tech Solutions. It covers all information security incidents, including:

- Data breaches (e.g., unauthorized access to customer data).
- Malware or ransomware attacks.
- Lost or stolen devices (e.g., laptops, USB drives).
- Phishing or social engineering attacks.
- System outages caused by security issues.

3. Definitions

- **Information Security Incident**: Any event that compromises the confidentiality, integrity, or availability of Tech Solutions' information or systems (e.g., a hacker accessing a server).
- **Incident Management**: The process of detecting, responding to, and recovering from security incidents.
- **Incident Response Team (IRT)**: The group responsible for handling incidents.

---

4. Roles and Responsibilities

The following roles are defined to ensure effective incident management. Each role has specific duties, and all personnel are trained to perform their tasks.

4.1 Chief Information Security Officer (CISO)

Responsibilities:

- Oversee the incident management program.
- Approve incident management policies and procedures.
- Ensure resources (e.g., tools, training) are available for the Incident Response Team.
- Communicate with senior management and external stakeholders (e.g., regulators) during major incidents.
- Review incident reports and lessons learned to improve processes.

Example: If a major data breach occurs, the CISO briefs the CEO and coordinates with legal counsel to notify regulators.

4.2 Information Security Manager

Responsibilities:

- Lead the Incident Response Team (IRT).
- Act as the primary point of contact for incident reporting (email: security@techsolutions.com).
- Prioritize incidents based on severity and impact (e.g., a ransomware attack is high priority).
- Coordinate with internal teams and external vendors during incidents.
- Maintain incident logs and documentation.
- Conduct post-incident reviews to identify improvements.

Example: When an employee reports a phishing email, the Information Security Manager investigates, isolates affected systems, and logs the incident.

4.3 Incident Response Team (IRT)

Responsibilities:

- Investigate and analyze security incidents.
- Contain and mitigate incidents (e.g., disconnect compromised servers).
- Recover systems and data (e.g., restore from backups).
- Document all actions taken during an incident.
- Participate in regular training and incident response drills.

Example: During a malware attack, the IRT scans systems, removes the malware, and resets passwords for affected accounts.

Team Members:

- IT Security Analyst (technical investigation and mitigation).
- System Administrator (system recovery and backups).
- Network Engineer (network monitoring and isolation).

4.4 Employees

Responsibilities:

- Report suspected security incidents immediately to security@techsolutions.com or via the internal reporting portal.
- Follow incident response procedures (e.g., do not attempt to fix issues themselves).
- Complete mandatory cybersecurity awareness training annually.

Example: An employee receives a suspicious email and reports it to the Information Security Manager instead of clicking the link.

4.5 Human Resources (HR) Department

Responsibilities:

- Handle incidents involving employee misconduct (e.g., sharing sensitive data).
- Coordinate disciplinary actions if needed.
- Support communication with affected employees during incidents.

Example: If an employee accidentally leaks customer data, HR works with the Information Security Manager to investigate and address the issue.

4.6 Customer Support Team

Responsibilities:

- Communicate with customers affected by incidents (e.g., notify them of a data breach).
- Follow scripts approved by the Information Security Manager and CISO.
- Log customer inquiries related to incidents.

Example: After a breach, the Customer Support Team sends an email to affected customers, explaining the issue and steps to protect their accounts.

4.7 Third-Party Vendors (e.g., Cloud Providers, IT Support)

Responsibilities:

- Report incidents involving their services to Tech Solutions' Information Security Manager.
- Assist the IRT in investigating and resolving incidents.
- Follow Tech Solutions' incident response procedures when handling our data.

Example: If our cloud provider detects unauthorized access to our servers, they notify us immediately and provide logs for investigation.

---

5. Incident Reporting Process

How to Report:

- **Internal**: Employees and contractors report incidents via:
  - Email: security@techsolutions.com
  - Internal portal: https://portal.techsolutions.com/security
  - Phone: +1-800-SEC-TECH (for urgent incidents)
- **External**: Vendors and customers report incidents to security@techsolutions.com.

What to Include:

- Description of the incident (e.g., "I saw unusual login attempts on my account").
- Time and date of the incident.
- Any evidence (e.g., screenshots, suspicious emails).

Example: An employee notices a strange pop-up on their computer and emails security@techsolutions.com with a screenshot and the time it appeared.

---

6. Incident Management Process

The following steps ensure incidents are handled efficiently:

1. **Detection and Reporting**:
   - Incidents are detected through monitoring tools (e.g., antivirus alerts) or employee reports.
   - All incidents are reported to the Information Security Manager.
2. **Triage and Prioritization**:
   - The Information Security Manager assesses the incident's severity:
     - **Low**: Minor issues (e.g., a single phishing email).

        - **Medium**: Potential risks (e.g., a lost laptop).
        - **High**: Major threats (e.g., a data breach or ransomware).
    - High-priority incidents are escalated to the CISO.
3. **Analysis and Containment**:
    - The IRT investigates the cause (e.g., checks logs for unauthorized access).
    - Immediate actions are taken to limit damage (e.g., isolate affected systems).
4. **Resolution and Recovery**:
    - The IRT resolves the issue (e.g., removes malware, restores data).
    - Systems are tested to ensure they're secure before resuming operations.
5. **Communication**:
    - Internal: The Information Security Manager updates relevant teams.
    - External: The CISO and Customer Support Team notify customers or regulators if required.
6. **Documentation and Lessons Learned**:
    - All actions are logged in the incident tracking system.
    - The IRT conducts a post-incident review to identify improvements (e.g., better email filters).

Example: A ransomware attack is detected (Step 1). The Information Security Manager labels it high-priority (Step 2). The IRT isolates the server and removes the malware (Step 3). Data is restored from backups (Step 4). The CISO notifies customers (Step 5). The team documents the incident and adds ransomware training for employees (Step 6).

---

7. Training and Competence

- **Initial Training**: All IRT members complete cybersecurity training (e.g., CompTIA Security+ or equivalent).
- **Ongoing Training**: Annual refreshers on new threats and incident response techniques.
- **Drills**: Quarterly incident response simulations (e.g., mock phishing attack).
- **Certifications**: IRT members are encouraged to pursue certifications like Certified Incident Handler (ECIH).
- **Employees**: All staff complete annual cybersecurity awareness training.

Example: The IT Security Analyst attends a workshop on ransomware response and practices handling a simulated breach during a drill.

---

8. Incident Management Objectives and Priorities

Objectives (agreed with management):

- Resolve high-priority incidents within 24 hours.
- Minimize downtime for critical systems (e.g., cloud services).
- Notify affected customers within 48 hours of a confirmed breach.
- Reduce repeat incidents by implementing lessons learned.

Priorities:

- Protect customer data and privacy.
- Maintain business continuity.
- Comply with legal and regulatory requirements (e.g., GDPR, CCPA).

Example: During a data breach, the IRT prioritizes securing customer data and notifying affected clients within 48 hours, as per the objectives.

---

9. Communication with Interested Parties

- **Internal**: The Information Security Manager updates employees via email or the company intranet.
- **External**: The CISO and Customer Support Team handle communications with customers, vendors, and regulators.
- **Escalation**: Major incidents are escalated to the CISO for stakeholder communication.

Example: After a phishing incident, the Information Security Manager emails all employees to warn them about suspicious emails, while the Customer Support Team informs affected clients.

---

10. Review and Improvement

- This document is reviewed annually or after major incidents.
- Feedback from the IRT and employees is used to improve processes.
- Lessons learned from incidents are incorporated into training and procedures.

Example: After a lost laptop incident, Tech Solutions updates its policy to require full-disk encryption on all devices.

---

11. Contact Information

- **Primary Contact**: Information Security Manager
  - Email: security@techsolutions.com
  - Phone: +1-800-SEC-TECH
- **Secondary Contact**: CISO
  - Email: ciso@techsolutions.com

---

12. Approval

Approved by: [CISO Name], Chief Information Security Officer
Date: May 05, 2025

TECH SOLUTIONS

Records of Security Event Processing Results

Example Entry

Event ID: SE-2025-001
Date and Time Reported: May 03, 2025, 09:15 AM
Reported By: Jane Doe, Customer Support Agent
Point of Contact: John Smith, Information Security Officer
Event Description: An employee received a phishing email disguised as a customer invoice, clicked a link, and entered login credentials on a fake website.
Detection Method: Employee reported the suspicious email to security@techsolutions.com after noticing the website looked unusual.
Triage and Prioritization:

- **Severity**: Medium (potential credential compromise but no evidence of further access).
- **Priority**: High (immediate action needed to secure account).
- **Potential Consequences**: Unauthorized access to employee account, potential data breach.
  Analysis:
- **Root Cause**: Employee clicked a phishing link due to lack of awareness about phishing tactics.
- **Affected Systems/Assets**: Employee's email account; no evidence of broader system compromise.
  Response Actions:
- **Actions Taken**:
  - Reset the employee's password and enabled two-factor authentication (2FA).
  - Ran a malware scan on the employee's laptop (no threats detected).
  - Blocked the phishing domain on the company firewall.
  - Notified the IT team to monitor for suspicious activity.
- **Personnel Involved**: John Smith (Information Security Officer), Alice Brown (IT Administrator).

- **Coordination**: Communicated with external cybersecurity vendor to analyze the phishing email's origin.
  Resolution Time Frame: 4 hours (from 09:15 AM to 01:15 PM on May 03, 2025).
  Outcome:
- **Status**: Resolved.
- **Impact**: No data loss or system compromise; minor disruption due to password reset.
  Lessons Learned:
- Employees need better training on identifying phishing emails.
- Consider implementing an email filtering tool to catch phishing attempts earlier.
  Documentation: Incident Report #IR-2025-001, email logs, vendor analysis report.
  Training/Certification Needs Identified: Schedule phishing awareness training for all employees; consider CompTIA Security+ certification for IT Administrator.
  Approval:
- **Reviewed By**: Sarah Lee, Chief Information Officer
- **Date Reviewed**: May 04, 2025