ISO 27001:2022 Checklist

Pacific Coast Data Center / Tony Smith / 20 Feb 2026

Complete

Score	119 / 127 (93.7%)	**Flagged items**	6	**Actions**	1

Site conducted	Unanswered
Site	Pacific Coast Data Center
Prepared by	Tony Smith
Date and Time	20.02.2026 08:00 PST
Location	8899 Pine Ln, Cotati, CA 94931, USA (38.3199567, -122.7195103)

Flagged items & Actions

6 flagged, 1 action

Flagged items

6 flagged, 1 action

Audit / 5. Leadership

5.1 (b) ensuring the integration of the information security management system requirements into the organization's processes;

More Work

To do | Priority: Low | Due: 02.03.2026 14:00 PST | Created by: SafetyCulture Staff

Direction of the organization

Let's discuss further on the plans for the proposed security policy and see if they fit our strategic direction

Audit / 5. Leadership

5.1 (d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

More Work

Audit / 8. Operation

The organization shall retain documented information of the results of the information security risk treatment.

More Work

Audit / 10. Improvement

10.2 (f) the nature of the nonconformities and any subsequent actions taken, and

More Work

Audit / 10. Improvement

10.2 (g) the results of any corrective action.

More Work

ISO 27001:2022 Risk Assessment Register / Table / Row 2

Risk Acceptance Approved?

No

Other actions

0 actions

Audit	5 flagged, 1 action, 93 / 100 (93%)
4. Context of the Organization	6 / 6 (100%)
4.1 Understanding the organization and its context	
The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	Done
4.2 Understanding the needs and expectations of interested parties	
The organization shall determine: 4.2 (a) interested parties that are relevant to the information security management system	Done
4.2 (b) the requirements of these interested parties relevant to information security	Done
4.2 (c) analysis of which of the interested party requirements must be addressed through the ISMS	Done
4.3 Determining the scope of the information security management system	
The organization shall determine the boundaries and applicability of the information security management system to establish its scope.	Done
4.4 Information security management system	
The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	Done
5. Leadership	2 flagged, 1 action, 8 / 10 (80%)
5.1 Leadership and commitment	
Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:	
5.1 (a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;	Done
5.1 (b) ensuring the integration of the information security	More Work

management system requirements into the organization's processes;	

To do | Priority: Low | Due: 02.03.2026 14:00 PST | Created by: SafetyCulture Staff

Direction of the organization

Let's discuss further on the plans for the proposed security policy and see if they fit our strategic direction

5.1 (c) ensuring that the resources needed for the information security management system are available;	Done
5.1 (d) communicating the importance of effective information security management and of conforming to the information security management system requirements;	More Work
5.1 (e) ensuring that the information security management system achieves its intended outcome(s);	Done
5.1 (f) directing and supporting persons to contribute to the effectiveness of the information security management system;	Done
5.1 (g) promoting continual improvement; and	Done
5.1 (h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	Done

5.2 Policy

Top management shall establish an information security policy that: **a) is appropriate to the purpose of the organization;** **b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;** **c) includes a commitment to satisfy applicable requirements related to information security; and** **d) includes a commitment to continual improvement of the information security management system.** **The information security policy shall:** **e) be available as documented information;** **f) be communicated within the organization; and** **g) be available to interested parties, as appropriate**	Done

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned, communicated, and done internally within the	Done

organization	
6. Planning	17 / 18 (94.44%)
6.1 Actions to address risks and opportunities	
6.1.1 General	
When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement	Done
6.1.1 (d) The organization shall plan actions to address these risks and opportunities; and	Done
6.1.1 (e) The organization shall plan how to: 1) integrate and implement these actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.	Done
6.1.2 Information security risk assessment	
6.1.2 (a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	Done
The organization shall define and apply an information security risk assessment process that:	
6.1.2 (b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;	Done
6.1.2 (c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners;	Done
6.1.2 (d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;	Done

2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk;	
6.1.2 (e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritize the analyzed risks for risk treatment.	Done

6.1.3 Information security risk treatment

The organization shall define and apply an information security risk treatment process to:

6.1.3 (a) select appropriate information security risk treatment options, taking account of the risk assessment results;	Done
6.1.3 (b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;	Done
6.1.3 (c) compare the controls determined in 6.1.3 (b) above with those in Annex A and verify that no necessary controls have been omitted;	Done
6.1.3 (d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3.b and c) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;	Done
6.1.3 (e) formulate an information security risk treatment plan; and	Done
6.1.3 (f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	Done

6.2 Information security objectives and plans to achieve them

The organization shall establish information security objectives at relevant functions and levels.	Done
The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and risk assessment and risk treatment results; d) be communicated and monitored; and e) be updated as appropriate.	Done

When planning how to achieve its information security objectives, the organization shall determine: **f) what will be done;** **g) what resources will be required;** **h) who will be responsible;** **i) when it will be completed; and** **j) how the results will be evaluated.**	Done
6.3 Planning of changes	
When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner	More Work
7. Support	24 / 24 (100%)
7.1 Resources	
The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	Done
7.2 Competence	
The organization shall:	
7.2 (a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;	Done
7.2 (b) ensure that these persons are competent on the basis of appropriate education, training, or experience;	Done
7.2 (c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and	Done
7.2 (d) retain appropriate documented information as evidence of competence.	Done
7.3 Awareness	
Persons doing work under the organization’s control shall be aware of:	
7.3 (a) the information security policy;	Done
7.3 (b) their contribution to the effectiveness of the information security management system, including the	Done

benefits of improved information security performance; and	
7.3 (c) the implications of not conforming with the information security management system requirements.	Done

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

7.4 (a) on what to communicate;	Done
7.4 (b) when to communicate;	Done
7.4 (c) with whom to communicate; and	Done
7.4 (d) who shall communicate	Done

7.5 Documented information

7.5.1 General

The organization's information security management system shall include:

7.5.1 (a) documented information required by this International Standard; and	Done
7.5.1 (b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.	Done

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

7.5.2 (a) identification and description (e.g. a title, date, author, or reference number);	Done
7.5.2 (b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and	Done
7.5.2 (c) review and approval for suitability and adequacy.	Done

7.5.3 Control of documented information

Documented information required by the information security management system and by this International Standard shall be controlled to ensure:

7.5.3 (a) it is available and suitable for use, where and when it is needed; and	Done
7.5.3 (b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).	Done

For the control of documented information, the organization shall address the following activities, as applicable:

7.5.3 (c) distribution, access, retrieval and use;	Done
7.5.3 (d) storage and preservation, including the preservation of legibility;	Done
7.5.3 (e) control of changes (e.g. version control); and	Done
7.5.3 (f) retention and disposition.	Done
Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.	Done

8. Operation

1 flagged, 8 / 9 (88.89%)

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1.	Done
The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.	Done
The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	Done
The organization shall ensure that outsourced processes are determined and controlled.	Done
The organization shall ensure that externally provided processes, products, or services that are relevant to the information security management system are controlled	Done

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2.a.	Done
The organization shall retain documented information of the results of the information security risk assessments.	Done

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.	Done
The organization shall retain documented information of the results of the information security risk treatment.	More Work

9. Performance evaluation

23 / 24 (95.83%)

9.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the information security performance and the effectiveness of the information security management system.	Done

The organization shall determine:

9.1 (a) what needs to be monitored and measured, including information security processes and controls;	Done
9.1 (b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;	Done
9.1 (c) when the monitoring and measuring shall be performed;	Done
9.1 (d) who shall monitor and measure;	Done
9.1 (e) when the results from monitoring and measurement shall be analyzed and evaluated; and	Done
9.1 (f) who shall analyze and evaluate these results.	Done

9.2 Internal audit

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:	Done

9.2 (a) conforms to 1) the organization's own requirements for its information security management system; and 2) the requirements of this International Standard;	Done
9.2 (b) is effectively implemented and maintained.	Done

The organization shall:

9.2 (c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;	Done
9.2 (d) define the audit criteria and scope for each audit;	Done
9.2 (e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;	Done
9.2 (f) ensure that the results of the audits are reported to relevant management; and	Done
9.2 (g) retain documented information as evidence of the audit programme(s) and the audit results.	Done

9.3 Management review

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.	Done

The management review shall include consideration of:

9.3 (a) the status of actions from previous management reviews;	Done
9.3 (b) changes in external and internal issues that are relevant to the information security management system;	Done
9.3 (c) feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 4) fulfilment of information security objectives;	Done
9.3 (d) feedback from interested parties;	Done

9.3 (e) results of risk assessment and status of risk treatment plan; and	Done
9.3 (f) opportunities for continual improvement.	Done
The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of the results of management reviews.	Done
9.3.2 inputs from interested parties need to be about their needs and expectations, and relevant to the ISMS	More Work
10. Improvement	2 flagged, 7 / 9 (77.78%)
10.1 Continual improvement	
The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	Done
10.2 Nonconformity and corrective action	
When a nonconformity occurs, the organization shall:	
10.2 (a) react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences;	Done
10.2 (b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur;	Done
10.2 (c) implement any action needed;	Done
10.2 (d) review the effectiveness of any corrective action taken; and	Done
10.2 (e) make changes to the information security management system, if necessary.	Done
Corrective actions shall be appropriate to the effects of the nonconformities encountered.	Done

The organization shall retain documented information as evidence of:

10.2 (f) the nature of the nonconformities and any subsequent actions taken, and	More Work
10.2 (g) the results of any corrective action.	More Work

ISO 27001:2022 Risk Assessment Register

1 flagged, 26 / 27 (96.3%)

	Risk ID	Scope Reference	Asset / Process	Information Type	Threat	Vulnerability	Impact (C)	Impact (I)	Impact (A)	Likelihood	Risk Level	Risk Criteria Met?	Risk Owner	Treatment Option	Selected Controls	Annex A Ref	Residual Risk	Risk Acceptance Approved?	Review Date
1	ISMS-RIS-001	Supplier on-boarding process (Scope: Procurement)	Supplier qualification records, PO documents, supplier emails	Operational Data	Unauthorized disclosure of supplier selection criteria; incorrect supplier info; delayed supplier documentation	New supplier onboarding process not documented; incomplete supplier QMS evidence; lack of formal secure file transfer	Moderate	High	Moderate	Likely	Moderate	Within Acceptance Criteria	Procurement Manager	Reduce	Formalize supplier onboarding SOP; require signed QMS evidence (ISO certs); secure file exchange (SFTP or encrypted email); supplier access controls; temporary increased incoming inspection; update PFMEA and Control Plan	A.8 (Asset management), A.12 (Operations security), A.15 (Supplier relationships)	Low (after controls & SOP)	Pending	02.03.2026
2	ISMS-RIS-002	HR / Ethics Reporting (Scope: Internal communications)	Anonymous reporting system & investigation records	Personal Data	Loss of anonymity leading to retaliation; tampering with reports; missed investigations	Investigation workflow unclear; limited separation of duties; logs not retained securely	Severe	High	Moderate	Likely	High	Within Acceptance Criteria	HR / Compliance Officer	Reduce	Update whistleblowing SOP with clear anti-retaliation controls; encrypt and restrict access to reports; implement audit logging; define retention; train HR/investigators; designate independent escalation path to Top Management	A.7 (Human resources), A.9 (Access control), A.16 (Information security incident management)	Low (after encryption, SOP, independent escalation)	No	02.03.2026

	Risk ID	Scope Reference	Asset / Process	Information Type	Threat	Vulnerability	Impact (C)	Impact (I)	Impact (A)	Likelihood	Risk Level	Risk Criteria Met?	Risk Owner	Treatment Option	Selected Controls	Annex A Ref	Residual Risk	Risk Acceptance Approved?	Review Date
3	ISMS-RIS-003	Production floor / Maintenance (Scope: Manufacturing Operations)	Production process data, calibration & maintenance records	Operational Data	Loss or corruption of process records causing inability to prove product conformity; delayed calibration information	Paper-based or local-only records; inconsistent back-up; insufficient version control for maintenance schedules	Moderate	High	Low	Possible	Moderate	Within Acceptance Criteria	Maintenance Manager / Quality Manager	Reduce	Digitize critical maintenance/calibration records; implement controlled document repository with versioning & backups; scheduled backups; access controls and MSA for measurement devices; validate data migration	A.8 (Asset management), A.12 (Operations security), A.14 (System acquisition & change)	Low (after digitization & backup)	Pending	02.02.2026

Completion

Comments/ Reconmmendations

We're well placed as far as working towards getting the third party certification for ISO 27001 is concerned. Everybody is working together and iAuditor has made our jobs simpler. I'll discuss more during our monthly meeting on Monday.

Name and Signature

Tony Smith
26.02.2026 10:22 PST