ISO 27001 Documentation Compliance Analysis Report

Generated on February 11, 2025

Executive Summary

94.9%

Overall Compliance Rate

78

Required Documents

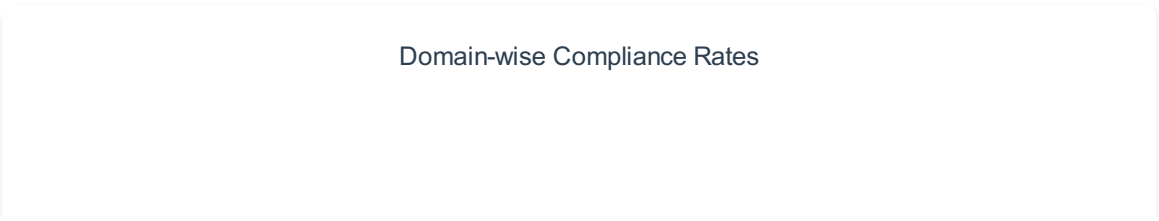
74

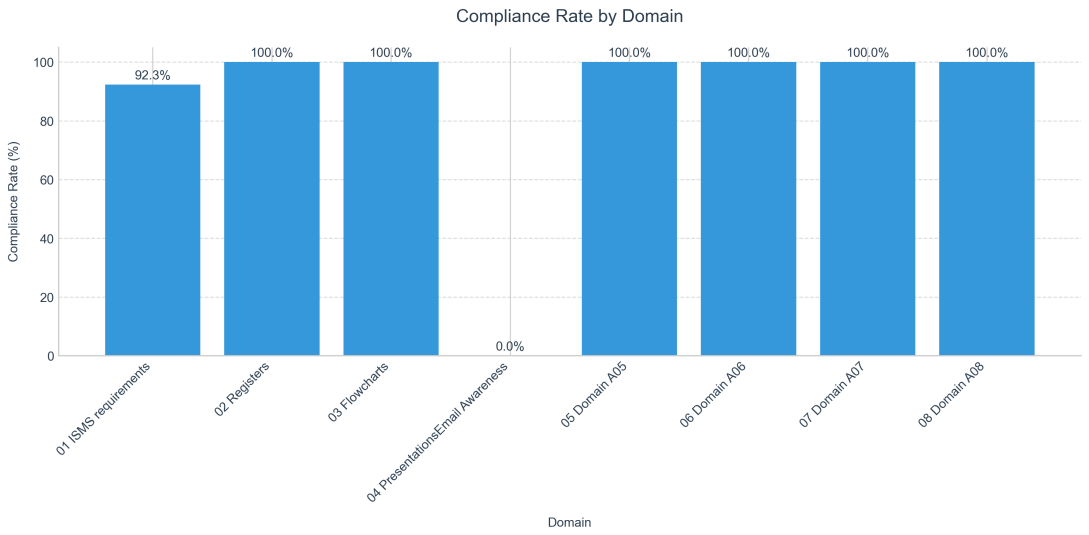
Existing Documents

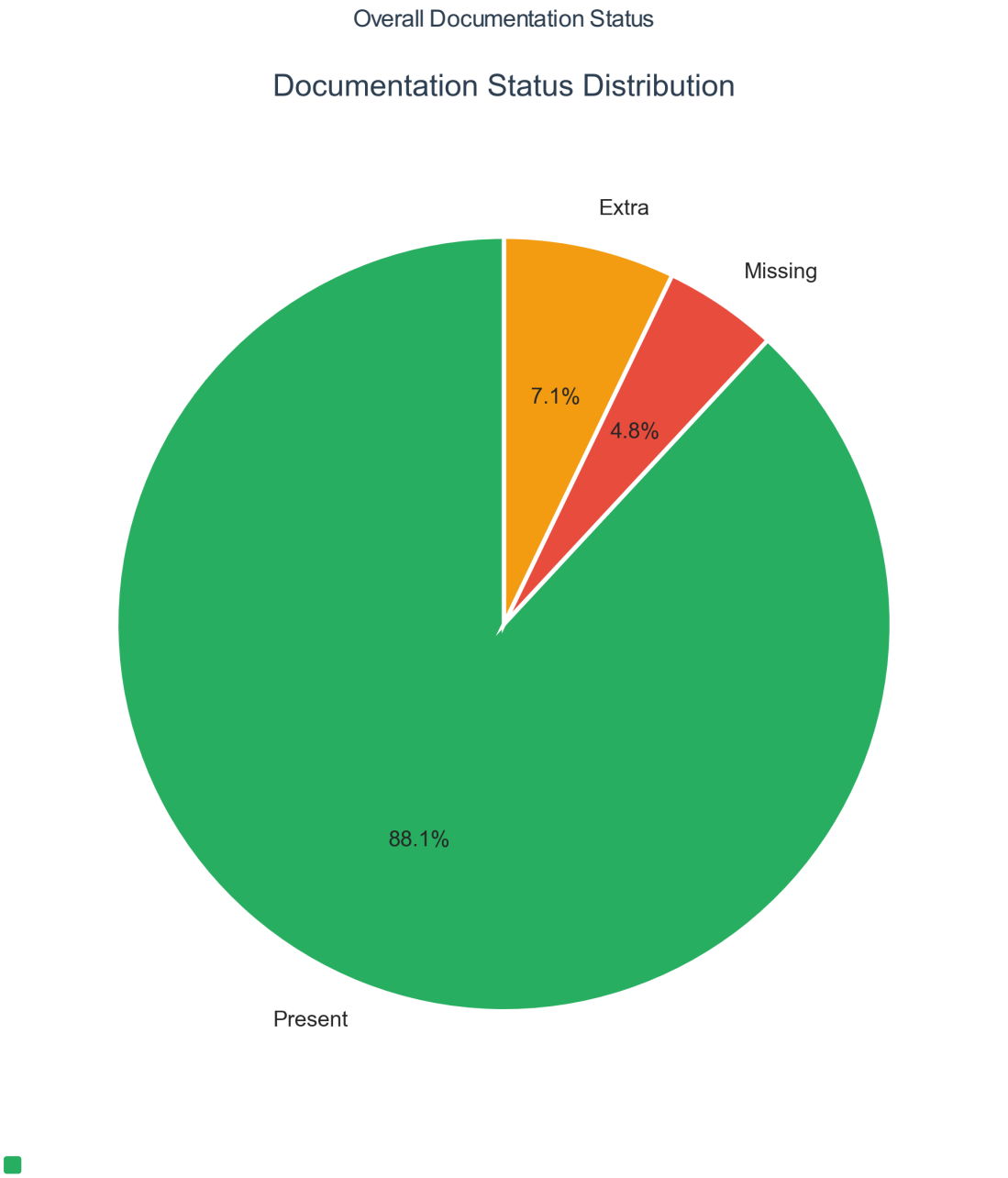
Domain-wise Analysis

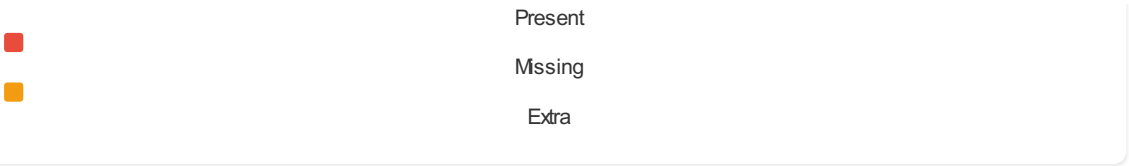
Domain	Compliance Rate	Required	Present	Missing
01 ISMS requirements	0.9%	13	12	1
02 Registers	1.0%	8	8	0
03 Flowcharts	1.0%	3	3	0
04 PresentationsEmail Awareness	0.0%	3	0	3
05 Domain A05	1.0%	17	17	0
06 Domain A06	1.0%	7	7	0
07 Domain A07	1.0%	7	7	0
08 Domain A08	1.0%	20	20	0

Compliance Visualization




Compliance Rate by Domain
Compliance Rate (%)
100
80
60
40
20
0
92.3%
100.0%
100.0%
0.0%
100.0%
100.0%
100.0%
100.0%
01 ISMS requirements
02 Registers
03 Flowcharts
04 PresentationsEmail Awareness
05 Domain A05
06 Domain A06
07 Domain A07
08 Domain A08
Domain


Overall Documentation Status
Documentation Status Distribution
Extra
Missing
7.1%
4.8%
88.1%
Present



Expert Analysis and Recommendations

ISO 27001 Documentation Analysis Report

1. Current Documentation Status Assessment

The current status of the ISO 27001 documentation is as follows:

> **Total Required Documents**: 78

> **Total Existing Documents**: 80

> **Compliance Rate**: 94.9%

Present Documents

- In total, **74 existing documented items** are actively utilized in compliance, providing a solid foundation for the ISMS (Information Security Management System).

Additional Documents

- There are **6 additional documents** that, while not required, could potentially enhance the organization's information security measures.

Missing Documents

- **4 essential documents** are missing, which could impact overall compliance and the effectiveness of the ISMS. ---

2. Key Areas of Concern Regarding Missing Documents

The analysis indicates significant gaps in specific domains, notably: - **Presentations & Awareness Materials**: - Missing: - **Email Awareness Poster** - **Information Security Awareness Training Presentation** - **Passwords Awareness Poster** - **ISMS Requirements**: - Missing: - **Information Security Policy**

Domain-Specific Gaps

- **01 ISMS requirements**: Lack of the main **Information Security Policy** may hinder the foundation of your security governance. - **04 Presentations**: The absence of awareness materials affects employee understanding and engagement with security practices. ---

3. Recommendations for Improvement

To enhance compliance and the robustness of the ISMS, the following steps are recommended:

Address Missing Documents:

Prioritize the creation or procurement of the missing **Information Security Policy** and essential awareness materials (posters and training presentation).

Review and Update Existing Documentation:

Conduct a periodic review of existing documents to ensure they remain relevant, current, and comprehensive.

This could include assessing and updating the risk assessment processes and security policies detailed in the present documentation.

Awareness and Training Programs:

Implement regular training sessions to ensure all employees are aware of information security protocols, including the use of newly developed materials.

Documentation Control Process:

Develop a clear plan for maintaining documentation, including scheduled reviews to assess relevance and compliance.

4. Potential Risks Associated with Missing Documentation

The absence of critical documents can expose the organization to various risks, including:

Compliance Risks:

Failing to maintain a comprehensive **Information Security Policy** may lead to noncompliance with ISO 27001 requirements, risking certification and regulatory issues.

Operational Risks:

Without adequate training and awareness materials, employees may not be wellinformed about security protocols, increasing the likelihood of security breaches due to human error.

Reputational Risks:

A perceived lack of commitment to information security can damage client and stakeholder trust and confidence.

Legal Risks:

Inadequate awareness and training could lead to violations of legal and regulatory requirements regarding data protection and privacy.

Summary

The current documentation status reflects a sound effort in establishing an ISO 27001-compliant ISMS framework, with a strong compliance rate. However, the identified missing documents – particularly the **Information Security Policy and awareness materials** – pose risks that could compromise the effectiveness and integrity of the ISMS. Taking proactive steps to address these gaps through routine audits, updates, and staff training will better position the organization to mitigate risks and reinforce its commitment to information security.

Missing Documents by Domain

Domain	Missing Documents
01 ISMS requirements	• information security policy.docx
04 PresentationsEmail Awareness	• email awareness poster.pdf • information security awareness training presentation.pptx • passwords awareness poster.pdf

Additional Documents Found

Document Name
.ds_store
cloudhub quality policy document.docx
isms-doc-a05-19-2 supplier selection process.docx
isms-doc-a05-7-1 threat intelligence policy.docx
isms-doc-a06-1-2 hr procedures for hiring, transfer & exit termination.docx
qv_001_information security policy.docx

Recommendations

- Create a timeline for implementing missing documentation
- Review and update existing documentation to ensure continued relevance
- Schedule regular documentation audits to maintain compliance
- Review additional documents found to determine if they should be incorporated into the documentation framework