2025

Seceon's Global Cybersecurity Framework Mapping Guide - IRDAI Compliance

Your essential resource to map your IRDAI compliance program goals to your cybersecurity program, controls, and Seceon's platform.

Achieving Continuous Compliance with Seceon

Seceon streamlines continuous compliance, integrating it seamlessly into daily security operations through automated workflows, real-time insights, and alignment with compliance frameworks. Our aiSIEM and aiXDR solutions empower organizations to meet regulatory requirements without overburdening IT and compliance teams.

Common Control Framework (CCF)

Seceon's Common Control Framework (CCF) is designed to support efficient compliance with multiple global standards. By consolidating security, privacy, and compliance mandates into a unified set of controls, CCF enables us to standardize compliance processes across varied services and products.

CCF Highlights

- **Unified Compliance:** CCF integrates requirements from multiple frameworks, including ISO 27001, SOC 2, HIPAA, NIST CSF 2.0, and PCI DSS, simplifying compliance management.
- **Mapped Controls:** Each control aligns with one or more regulatory standards, allowing a single control to satisfy several compliance mandates.
- **Domain Structure:** CCF organizes controls into domains that cover key areas of security and compliance.
- **Three-Tiered Control System:** CCF categorizes controls into People, Process, and Technology.
  - **People Controls:** Address training, awareness, and organizational structure.
  - **Process Controls:** Cover documented procedures, manual rule enforcement, and risk assessment.
  - **Technology Controls:** Govern data processing, IT asset management, and network security.

Leveraging CCF along with Seceon's robust tools, organizations can generate interactive compliance reports for frameworks like HIPAA, NIST CSF, and PCI-DSS, providing audit-ready documentation for diverse regulatory needs.

Key Compliance-Enhancing Features on Seceon's Platform

1.Centralized Visibility and Monitoring: Our platform collects and correlates data from diverse sources, including firewalls, intrusion detection systems, servers, and endpoints, delivering unified visibility across the network.

2.Threat Detection and Incident Response: Powered by machine learning, Seceon's advanced threat detection swiftly identifies unusual patterns or potential incidents, enabling rapid incident response.

3.Continuous Compliance Reporting: Equipped with robust reporting tools, Seceon's platform generates detailed, framework-specific reports to simplify audits.

4.Log Management and Audit Trails: Comprehensive log collection and management support Seceon's commitment to rigorous auditing standards.

5.Risk Management Support: The platform's Risk Assessment (RA) tools analyze data to pinpoint and prioritize potential threats, fostering a proactive security posture.

Visit the official IRDAI

https://irdai.gov.in/

IRDAI Compliance:

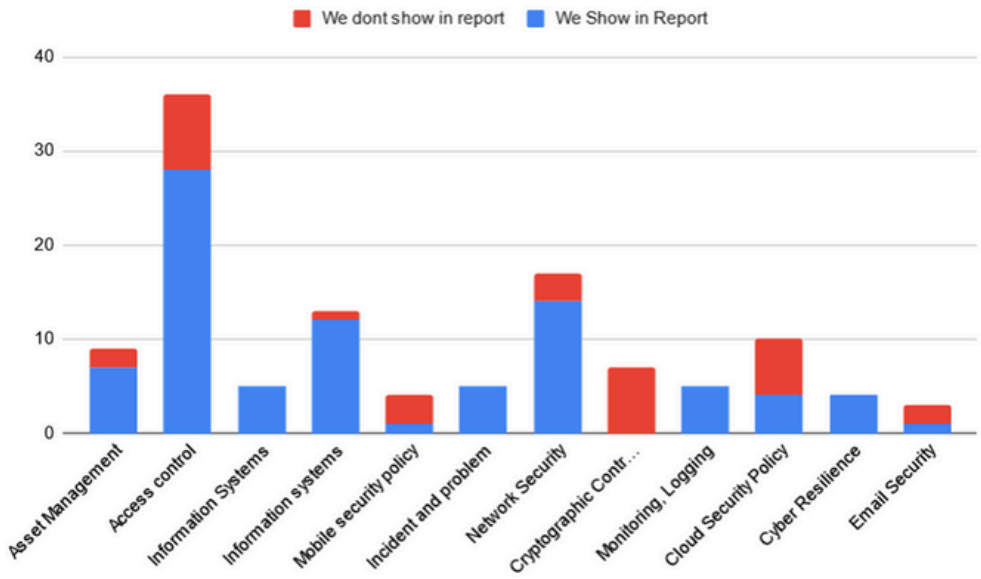
The **IRDAI Cyber Security Framework (CSF)** provides guidelines for enhancing the cyber resilience of insurance companies in India. It requires insurers to establish a robust cybersecurity policy approved by their board, focusing on protecting sensitive customer data and critical systems. The framework mandates regular risk assessments, implementation of security controls like encryption, secure access, and network monitoring, and development of an incident response plan to handle cyber threats effectively. By enforcing these measures, the IRDAI CSF aims to safeguard the insurance sector against evolving cyber risks and ensure the stability and trust of the ecosystem.



Seceon's approach is closely aligned with IRDAI CSF's core functions, emphasizing enhanced resilience and readiness for regulatory compliance. Using our Open Threat Management (OTM) platform, we focus extensively on technology controls within the IRDAI CyberSecurity framework, providing a measurable demonstration of compliance against specific technical controls. This focus includes automated threat detection, incident response, and continuous monitoring capabilities that serve as critical components of an organization's cybersecurity program.

While our reports and KPIs concentrate on technology controls, it is important to note that people, process, and governance-related controls—which often involve detailed documentation and procedural evidence—are outside the primary scope of our automated compliance reports. This distinction ensures that Seceon's OTM platform directly supports the operational and technical facets of cybersecurity, allowing organizations to focus resources effectively across their broader cybersecurity program.

IRDAI Core Requirements and Coverage:



IRDAI Mapping Table:

No.	Domain Title	Number of Total Controls	Number of Technical Controls	Technology Controls Mapped to Seceon	Seceon CCF Controls
1	Asset Management	58	9	1.1, 1.2.3, 1.2.2.2,	DM-02 CFM-07,IAM-13, IAM-25, IAM-25
2	Access control	57	36	2.1, 2.2, 2.3, 2.5, 2.6, 2.6.1, 2.7, 2.8	IAM-01, IAM-04, IAM-11, IAM-13, IAM-16, IAM-19, IAM-23, IAM-25, IAM-29, IAM-30, IAM-33, IAM-35, CFM-05, VM-09.

3	Information Systems acquisition and development	17	5	3.1.1.1, 3.2.4	CFM-01, CFM-09, SM-25
4	Information systems maintenance	28	15	4.3, 4.4, 4.5	SM-01, SM-11, SM-26, SM-31, PS-01, VM-09, CFM-05, IR-01, MDM-03.
5	Mobile security policy	7	4	5.1, 5.3	MDM-03, IAM-29
6	Incident and problem management	14	6	6.1, 6.2, 6.4	CFM-01, SM-01, SM-25, IR-01, IR-03, IR-04, IR-05
7	Network Security	26	17	7.1, 7.2	NO-01, NO-08, NO-16, NO-18, SM-15, SM-26, IAM-13, IAM-14, CFM-01.
8	Cryptographic Controls	7	7	Not Applicable	Not Applicable
9	Monitoring, Logging and Assessment	13	4	9.2, 9.5.1	SM-01, SM-31, IR-01.
10	Cloud Security Policy	14	10	10.1.1, 10.1.3	IAM-14, IAM-30, NO-01,SM-26,
11	Cyber Resilience	13	10	11.1, 11.2, 11.2.1, 11.2.3, 11.2.4, 11.2.5, 11.2.7	IR-01, IR-02, IR-03, IR-04, IR-05, PS-02, VM-03, SM-01, CFM-01.

12	Email Security	4	3	Not Applicable	Not Applicable

About Seceon

Seceon enables MSPs, MSSPs, and IT teams to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon augments and automates MSP, MSSP, and IT security services with an AI and ML-powered aiSIEM and aiXDR platform. It delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It's all enriched and analyzed in real-time with threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 640 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 8,800 clients.

Learn more about Seceon

Schedule a Demo www.seceon.com/contact/



© 2025 Seceon Inc. All rights reserved. aiSIEM, aiXDR, aiMSSP are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.