Ogma

CONFIDENTIAL

Firewall Compliance Report

FortiGate-60F (fortigate) — FortiGate Configuration Audit

COMPLIANCE SCORE	48% — FAIR
DEVICE	FortiGate-60F (fortigate)
IP ADDRESS	N/A
HOSTNAME	FortiGate-60F
FIRMWARE	N/A
FINDINGS	1 Critical · 18 High · 27 Medium · 10 Low
AUDIT MODE	upload
REPORT ID	FA-8
REPORT DATE	08 Apr 2026 12:22 UTC

Table of Contents

SD-WAN	2 findings

RISK QUANTIFICATION

Compliance Penalty Exposure	
Estimated Breach Cost	
Downtime Risk Assessment	

COMPLIANCE GAP ANALYSIS

CIS FortiGate Benchmark	58 gaps
ISO 27001	45 gaps
PCI-DSS	43 gaps
CERT-In	20 gaps
RBI IT Framework	7 gaps
SEBI CSCRF	3 gaps
DPDPA 2023	2 gaps

Executive Summary

Device: FortiGate-60F (fortigate) | **IP:** N/A | **Hostname:** FortiGate-60F | **Firmware:** N/A | **Mode:** upload

48%

Compliance Score — Fair

1	18	27	10
CRITICAL	HIGH	MEDIUM	LOW

⚠ **Firmware Version Unavailable:** The firmware version could not be determined from the provided configuration. This limits the accuracy of CVE correlation and version-specific benchmark checks. We strongly recommend providing the exact FortiOS/PAN-OS version string for a more precise assessment covering known vulnerabilities and vendor-specific hardening guidance.

Overall Risk Assessment

IMMEDIATE BREACH RISK: Your firewall has 1 critical vulnerability that could be exploited today. Each one represents a direct path an attacker can take to compromise your network without sophisticated tools or techniques. Remediation within 24 hours is non-negotiable.

HIGH EXPOSURE: 18 high-severity misconfigurations create significant attack surface. Any determined adversary scanning your perimeter will find multiple entry points. These must be addressed within the first 30 days to materially reduce risk.

Your firewall is functioning below acceptable security thresholds. Multiple attack vectors are available to threat actors. Without urgent remediation, a security incident is a matter of when, not if.

Top Attack Scenarios Based on Findings

The following attack chains are constructed from your actual audit findings. Each represents a realistic path a threat actor could take today.

1. VPN Gateway Compromise

Attack chain: Attacker discovers exposed VPN portal → brute-forces credentials (no 2FA) → gains admin access → pivots to internal network

Impact: Full network access, credential theft, data exfiltration, ransomware deployment

2. Malware Delivery via Uninspected Traffic

Attack chain: Malware-laden email passes through uninspected → endpoint executes payload → C2 callback succeeds (no IPS/app-control to block) → encrypted C2 channel evades all detection

Impact: Ransomware infection, data theft, business disruption, lateral movement to critical assets

3. Firewall Management Plane Takeover

Attack chain: Attacker scans management interface → finds exposed admin portal (no local-in policy) → brute-forces admin credentials (no 2FA / no trusted-host restriction) → disables logging to cover tracks → modifies firewall rules to allow persistent access

Impact: Complete perimeter control loss, invisible persistence, all traffic reroutable, total network compromise

Key Business Impacts

DATA BREACH
Exposure of customer PII, financial records, and intellectual property. DPDPA penalties up to ₹250 Cr.

⚠

OPERATIONAL DISRUPTION
Ransomware, DDoS, or config wipe can halt business operations for days to weeks.

⚖

REGULATORY PENALTIES
Non-compliance with CERT-In, DPDPA, PCI-DSS, RBI, SEBI frameworks. Fines, license risk.

REPUTATION DAMAGE
Loss of customer trust, partner confidence, and market position following a public breach.

⚠ Security Reality Check

- ✖ Traffic is passing through your firewall like a router, not a firewall. Policies exist but lack the security profiles (IPS, AV, web filter) that actually inspect and block threats.
- ✖ If a breach happens today, you will not know what happened. There is no centralised log collection, which means no forensics, no alerting, and no compliance evidence.
- ✖ The management plane is directly exposed to takeover. Without local-in policies restricting management access and without admin 2FA, anyone who can reach the management IP can attempt to brute-force their way in.
- ✖ This is pre-2010 level security. Without IPS or antivirus inspection, the firewall cannot detect known exploits, malware, or command-and-control traffic. Modern threats will pass through completely undetected.
- ✖ There is no high-availability configuration. A single hardware failure will take your entire network offline with no automatic failover.

Priority Actions & Remediation Roadmap

⚠ Immediate Actions — Complete Within 24–48 Hours

These findings represent the highest-risk items that could be actively exploited. Prioritise these above all other IT work.

PCOV-006 **Accept Policies Without Any Security Profiles** — CRITICAL

→ Single point of failure — one device failure takes the entire network offline.

Apply a minimum set of security profiles (AV, IPS, web filter, SSL inspection) to every accept policy.

SYS-002 **Strong Crypto Not Enabled** — HIGH

→ Remote access gateway vulnerability — direct path to internal network compromise.

Enable strong crypto to enforce modern cipher suites (AES-128/256, SHA-256+).

```
config system global set strong-crypto enable end
```

POL-001 **Overly Permissive Rules (Any/Any/Any)** — HIGH

→ Remote access gateway vulnerability — direct path to internal network compromise.

Restrict source/destination addresses and services to the minimum required. Eliminate any/any/any accept rules.

```
config firewall policy edit set srcaddr set dstaddr set...
```

POL-002 **Policies Without Security Profiles** — HIGH

→ Remote access gateway vulnerability — direct path to internal network compromise.

Apply UTM security profiles (antivirus, IPS, web filter) to all accept policies.

```
config firewall policy edit set utm-status enable set av-profile "default" set ips-sensor...
```

ADM-001 **Default Admin Username** — HIGH

→ Security gap that increases overall attack surface.

Rename default admin accounts to unique names to prevent targeted brute-force attacks.

```
config system admin rename admin to end
```

30-Day Hardening Roadmap

Medium-severity findings that strengthen defence-in-depth. Schedule these in your next change window cycle.

SYS-008 **Anti-Replay Protection Not Strict** — MEDIUM

Enable strict anti-replay protection.

```
config system global set anti-replay strict end
```

POL-004 **Policies Without Logging** — MEDIUM

Enable traffic logging (at least "utm" or "all") on all active policies.

```
config firewall policy edit set logtraffic all next end
```

POL-005 **Policies Allowing All Services** — MEDIUM

Restrict services to specific ports/protocols required for business functions.

```
config firewall policy edit set service HTTP HTTPS DNS next end
```

TF-001 **No External Threat Intelligence Feeds Configured** MEDIUM

Integrate third-party threat feeds (STIX/TAXII, Ogma TI, MISP) via system external-resource for enhanced IOC blocking beyond FortiGuard.

```
config system external-resource edit "ogma-ti-feed" set type flat-file set resource...
```

SDWAN-001 **SD-WAN Enabled Without Health Checks** MEDIUM

Configure SD-WAN health checks to monitor link latency, jitter, and packet loss.

```
config system sdwan config health-check edit "internet-check" set server "8.8.8.8" set protocol...
```

ADM-004 **Password Expiration Not Configured** MEDIUM

Configure password expiration (max 90 days) for all admin accounts.

```
config system admin edit set password-expire 2099-12-31 00:00:00 next end
```

ADM-006 **Admin Accounts Without Password Policy** MEDIUM

Enable the global password policy or assign per-admin password policies.

```
config system password-policy set status enable set min-length 12 set min-upper-case-letter 1 set...
```

SYS-001 **Admin Session Timeout** MEDIUM

Set admin timeout to 5 minutes for compliance.

```
config system global set admintimeout 5 end
```

SYS-010 **Admin Lockout Not Configured** MEDIUM

Set admin lockout threshold to 3-5 failed attempts.

```
config system global set admin-lockout-threshold 3 set admin-lockout-duration 300 end
```

SYS-007 **USB Auto-Install Enabled** MEDIUM

Disable USB auto-install to prevent unauthorized firmware or configuration overwrites via physical access.

```
config system auto-install set auto-install-config disable set auto-install-image disable end
```

90-Day Maturity Roadmap

Low-priority hardening and best-practice items. Include in quarterly security review and ongoing improvement plans.

SDWAN-002 **SD-WAN SLA Targets Not Defined** LOW

Define SLA targets in SD-WAN service rules for performance-based link steering.

SYS-005 **Default HTTPS Admin Port** LOW

Change the admin HTTPS port to a non-standard port (e.g., 8443).

CRT-001 **Self-Signed Admin GUI Certificate** LOW

Install a CA-signed certificate for the admin GUI to prevent MITM attacks and browser warnings.

SYS-003 **Pre-Login Banner Not Configured** LOW

Configure a pre-login banner with legal warning text.

SYS-004 **Post-Login Disclaimer Not Configured** LOW

Configure a post-login disclaimer banner.

NTP-002 **Using Default FortiGuard NTP Only** LOW

Add custom NTP servers (e.g., time.google.com, time.nist.gov) alongside FortiGuard.

NTP-003 **NTP Authentication Not Enabled** LOW

Enable NTP authentication with MD5/SHA1 keys.

DNS-002 **DNS Over TLS Not Configured** LOW

Enable DNS over TLS to encrypt DNS queries.

WF-004 **Safe Search Not Enforced** LOW

Enable Safe Search enforcement in web filter profiles.

APPCTRL-003 **Application Control Not Using Deep Inspection** LOW

Enable deep application inspection for better detection of evasive applications.

Scoring Methodology

The compliance score is calculated using a **weighted deduction model**. Each failed check deducts points proportional to its severity. The deduction is measured against a baseline of 2,000 maximum impact points.

Severity Weights

SEVERITY	POINTS DEDUCTED PER FINDING	RATIONALE
CRITICAL	**50 points**	Directly exploitable; immediate breach risk
HIGH	**30 points**	Significant attack surface; requires prompt action
MEDIUM	**15 points**	Defence-in-depth gap; exploitable in combination
LOW	**5 points**	Hardening recommendation; minimal direct risk

Formula

```
Impact = (Critical × 50) + (High × 30) + (Medium × 15) + (Low × 5)
Score = 100 − (Impact ÷ 2000 × 100)
```

Baseline: 2,000 points. Score is clamped to 0–100%. A score of 100% means zero failed checks. A score of 0% means the cumulative impact has reached or exceeded the baseline threshold.

Your Calculation

```
Impact = (1 × 50) + (18 × 30) + (27 × 15) + (10 × 5) = 1045
Score = 100 − (1045 ÷ 2000 × 100) = 48%
```

Score Bands

Excellent	Good	Fair	Poor
80–100%	60–79%	40–59%	0–39%

Administrator Accounts (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
ADM-001	Default Admin Username Related: ADM-002, ADM-004, ADM-006, SYS-001, SYS-010, SYS-005, CRT-001	HIGH	Admin accounts using default "admin" username detected: admin. CLI: `config system admin rename admin to end` CERT-In, PCI-DSS 8.5, ISO 27001 A.9.4.3, DPDPA 2023 Sec 8	Rename default admin accounts to unique names to prevent targeted brute-force attacks.

Interface Security

✓ All checks passed in this category.

Global System Settings (5 findings)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
SYS-002	Strong Crypto Not Enabled Related: POL-001, POL-005	HIGH	Strong crypto is disabled. Weak ciphers (DES, 3DES, RC4) may be negotiated for management and VPN sessions. CLI: `config system global set strong-crypto enable end` CERT-In, PCI-DSS 4.1, ISO 27001 A.10.1.1, RBI IT Framework	Enable strong crypto to enforce modern cipher suites (AES-128/256, SHA-256+).
SYS-003	Pre-Login Banner Not Configured	LOW	No pre-login legal banner configured. A warning banner is required by most compliance frameworks to assert authorized-use-only. CLI: `config system global set pre-login-banner enable set...` PCI-DSS 2.2, ISO 27001 A.9.1.1, CERT-In	Configure a pre-login banner with legal warning text.
SYS-004	Post-Login Disclaimer Not Configured	LOW	No post-login disclaimer configured. CLI: `config system global set post-login-banner enable set...` ISO 27001 A.9.1.1	Configure a post-login disclaimer banner.
SYS-007	USB Auto-Install Enabled	MEDIUM	USB auto-install enabled for: auto-install-config, auto-install-image. Physical access could allow unauthorized firmware or config replacement. CLI: `config system auto-install set auto-install-config disable set...` ISO 27001 A.11.2.1, PCI-DSS 9.1	Disable USB auto-install to prevent unauthorized firmware or configuration overwrites via physical access.
SYS-009	Strict Dirty Session Check Disabled	MEDIUM	Strict dirty session check is disabled. This weakens session integrity validation for firewall policies. CLI: `config system global set strict-dirty-session-check enable end` ISO 27001 A.13.1.1	Enable strict dirty session checking.

Firewall Policies (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
POL-002	Policies Without Security Profiles Related: SEC-002, IPS-001, IPS-004, FG-001, PCOV-002, SYS-008	HIGH	11 active accept policy(ies) have no security profiles (AV, IPS, Web Filter): Policy Cyclades-Wifi-LAN (Cyclades-Wifi-LAN), Policy LAN-Cyclades-WiFi (LAN-Cyclades-WiFi), Policy Ogma-WiFi-LAN (Ogma-WiFi-LAN), Policy LAN-Ogma-WiFi (LAN-Ogma-WiFi), Policy Internet (Internet), Policy vpn_DC-CTRLS_remote_0 (vpn_DC-CTRLS_remote_0), Policy vpn_DC-CTRLS_remote_1 (vpn_DC-CTRLS_remote_1), Policy vpn_DC-CTRLS_remote_2 (vpn_DC-CTRLS_remote_2), Policy vpn_DC-CTRLS_local_0 (vpn_DC-CTRLS_local_0), Policy vpn_DC-CTRLS_local_1 (vpn_DC-CTRLS_local_1) ... and 1 more. CLI: `config firewall policy edit set utm-status enable set...` PCI-DSS 5.1, ISO 27001 A.12.2.1, CERT-In	Apply UTM security profiles (antivirus, IPS, web filter) to all accept policies.

VPN Configuration

✓ All checks passed in this category.

Logging & Monitoring (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
LOG-001	No Remote Syslog Configured Related: POL-004, LOG-002, LOG-004	HIGH	Remote syslog is not configured. Logs stored only on the firewall can be lost during a compromise or hardware failure. CLI: `config log syslogd setting set status enable set server ...` CERT-In 180-day log retention, PCI-DSS 10.5.4, ISO 27001 A.12.4.1, RBI IT Framework, SEBI CSCRF	Configure remote syslog to a centralized SIEM or log management platform.

NTP Configuration (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
NTP-002	Using Default FortiGuard NTP Only Related: NTP-003	LOW	NTP is configured to use FortiGuard NTP servers only. Consider adding additional authoritative NTP sources for redundancy. CLI: `config system ntp set type custom config ntpserver edit 1 set...` PCI-DSS 10.4	Add custom NTP servers (e.g., time.google.com, time.nist.gov) alongside FortiGuard.

DNS Configuration

✓ All checks passed in this category.

Password Policy (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
PWD-001	Password Policy Not Enabled	HIGH	Global password policy is not enabled. Weak passwords can be set without enforcement. CLI: `config system password-policy set status enable set min-length 12 set...` PCI-DSS 8.3.6, ISO 27001 A.9.4.3, CERT-In, RBI IT Framework	Enable the global password policy with strong requirements.

SNMP Configuration

✓ All checks passed in this category.

High Availability

✓ All checks passed in this category.

API User Security (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
API-001	API Users Without Trusthost	HIGH	1 API user(s) have no trusthost restriction: test-api. API tokens can be used from any IP. CLI: `config system api-user edit config trusthost edit 1 ...` PCI-DSS 7.1, ISO 27001 A.9.4.1, CERT-In	Configure trusthost restrictions for all API users to limit access to known management IPs.

Certificate Management

✓ All checks passed in this category.

Routing & Network (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
NET-002	Static Routes Without Comments	INFO	1 static route(s) have no comment/ description: Route ? (?). Comments aid troubleshooting and change management. CLI: `config router static edit set comment "Description of route...` ISO 27001 A.12.1.2	Add comments to all static routes describing their purpose.

Security Profiles

✓ All checks passed in this category.

Local-In Policies (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
LIP-001	No Local-In Policies Configured	HIGH	No local-in policies are configured. The management plane is unprotected — any source IP can attempt to reach management services (HTTPS, SSH, SNMP) on the firewall interfaces. CLI: `config firewall local-in-policy edit 1 set intf "wan1" set srcaddr...` CERT-In, PCI-DSS 1.2.1, ISO 27001 A.13.1.1	Create local-in policies to restrict management-plane access to trusted administrator hosts/subnets only.

Web Filter (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
WF-002	Web Filter Not Using FortiGuard Category Filtering Related: WF-003, PCOV-003, WF-004	MEDIUM	Web filter profiles are not using FortiGuard category-based filtering, relying only on static URLs or keywords. PCI-DSS 1.3.5, ISO 27001 A.13.1.3	Enable FortiGuard category-based filtering in web filter profiles for comprehensive URL classification.

Intrusion Prevention (IPS)

✓ All checks passed in this category.

DNS Security (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
DNSSEC-001	FortiGuard DNS Filtering Not Enabled Related: DNSSEC-002, DNS-002	HIGH	FortiGuard DNS filtering and DNS-over-TLS are not enabled. DNS queries are unencrypted and malicious domain requests are not blocked at the DNS layer. CLI: `config system dns set dns-over-tls enable end` PCI-DSS 1.3.5	Enable FortiGuard DNS filtering and DNS-over-TLS for secure DNS resolution and domain-level threat blocking.

Antivirus (Deep Analysis) (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
AV-002	Antivirus Not Scanning All Protocols Related: PCOV-001, AV-003, AV-004, AV-005, FG-003	HIGH	Antivirus profiles are not configured to scan all key protocols (HTTP, SMTP, POP3, IMAP, FTP). Malware can bypass scanning via unprotected protocols. PCI-DSS 5.1, ISO 27001 A.12.2.1, CERT-In	Enable antivirus scanning on all protocols in every antivirus profile.

SSL/SSH Inspection (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
SSL-002	Using Certificate Inspection Only Related: SSL-003, PCOV-005, APPCTRL-003	MEDIUM	No SSL inspection profile uses deep inspection. Certificate inspection cannot decrypt and inspect HTTPS payload — encrypted threats will pass through. CLI: `config firewall ssl-ssh-profile edit "deep-inspect" config https ...` PCI-DSS 4.1, ISO 27001 A.18.1.5	Enable deep SSL inspection for critical segments. Certificate inspection misses encrypted threats.

Application Control (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
APPCTRL-002	High-Risk Application Categories Not Blocked Related: PCOV-004	MEDIUM	Application control profiles do not block high-risk categories (P2P, proxy, botnet). These categories are commonly used for data exfiltration and C&C communication. PCI-DSS 1.2.1, ISO 27001 A.13.1.3	Block P2P, proxy, and botnet application categories in application control profiles.

FortiGuard Services (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
FG-002	FortiGuard Update Server Not Reachable or Auto-Update Disabled	MEDIUM	FortiGuard update server is unreachable or automatic updates are disabled. Security definitions will become stale. CLI: `config system fortiguard set auto-firmware-upgrade enable end` PCI-DSS 5.2	Ensure the firewall can reach FortiGuard update servers. Enable automatic updates for all security services.

Threat Intelligence Feeds (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
TF-001	No External Threat Intelligence Feeds Configured	MEDIUM	No external threat intelligence feeds (STIX/TAXII, IP blocklists, domain feeds) are configured. The firewall relies solely on FortiGuard for IOC intelligence. CLI: `config system external-resource edit "ogma-ti-feed" set type...` CERT-In, ISO 27001 A.12.2.1	Integrate third-party threat feeds (STIX/TAXII, Ogma TI, MISP) via system external-resource for enhanced IOC blocking beyond FortiGuard.

Policy Security Coverage (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
PCOV-006	Accept Policies Without Any Security Profiles	CRITICAL	11 accept policy(ies) have zero UTM/security profiles applied. Traffic matching these policies receives no security inspection whatsoever. PCI-DSS 5.1, PCI-DSS 11.4, ISO 27001 A.12.2.1	Apply a minimum set of security profiles (AV, IPS, web filter, SSL inspection) to every accept policy.

DoS Protection (1 finding)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
DOS-001	No DoS Policies Configured	MEDIUM	No DoS protection policies are configured. The firewall has no dedicated defence against volumetric or protocol-based denial-of-service attacks. CLI: `config firewall DoS-policy edit 1 set interface "wan1" set srcaddr...` ISO 27001 A.13.1.1	Create DoS policies to protect critical interfaces and services against flood attacks.

SD-WAN (2 findings)

ID	FINDING	SEVERITY	DETAILS	RECOMMENDATION
SDWAN-001	SD-WAN Enabled Without Health Checks Related: HA-001	MEDIUM	SD-WAN is enabled but no health checks (SLA probes) are configured. Link quality cannot be monitored and failover will not trigger on degradation. CLI: `config system sdwan config health-check edit "internet-check" ...` ISO 27001 A.13.1.1	Configure SD-WAN health checks to monitor link latency, jitter, and packet loss.
SDWAN-002	SD-WAN SLA Targets Not Defined	LOW	SD-WAN SLA targets (latency, jitter, packet loss thresholds) are not defined. Link selection cannot be performance-based. ISO 27001 A.13.1.1	Define SLA targets in SD-WAN service rules for performance-based link steering.

Risk Quantification

Estimated financial and operational exposure based on audit findings, mapped to industry benchmarks and Indian regulatory frameworks.

Compliance Penalty Exposure

CIS FortiGate Benchmark MEDIUM

58 gaps. CIS Benchmark deviations increase attack surface. While not regulatory, many cyber-insurance policies require CIS compliance.

ISO 27001 MEDIUM

45 gaps. Could result in non-conformity during surveillance audit, potential certification suspension.

PCI-DSS HIGH

43 gaps. PCI-DSS non-compliance penalties range from $5,000 to $100,000/month from card brands, plus liability for fraudulent transactions.

CERT-In HIGH

20 gaps. CERT-In Directions 2022 mandate 6-hour incident reporting and 180-day log retention. Non-compliance can result in imprisonment up to 1 year and fines.

RBI IT Framework HIGH

7 gaps. RBI IT Framework non-compliance can lead to restrictions on business operations and penalties under Banking Regulation Act.

SEBI CSCRF MEDIUM

3 gaps. SEBI CSCRF mandates quarterly vulnerability assessments. Non-compliance can trigger show-cause notices and trading restrictions.

DPDPA 2023 HIGH

2 gaps. Digital Personal Data Protection Act 2023 penalties up to ₹250 Crore per incident for significant data fiduciaries.

Estimated Breach Cost

₹22.4 Crore HIGH RISK

Based on IBM Cost of a Data Breach Report 2024 (India average: ₹19.5 Crore), adjusted by your security posture score (48%). Severity multiplier: 1.15x. Includes direct costs (forensics, notification, legal) and indirect costs (business disruption, reputation, customer churn).

Downtime Risk Assessment

HIGH

Multiple infrastructure resilience gaps detected: no high-availability (single point of failure); no centralised logging (delayed incident detection). Estimated MTTR for a significant incident: 24-72 hours. Business impact at typical enterprise downtime cost of ₹10-50 Lakh/hour could exceed ₹2.4 Crore for a single extended outage.

Compliance Gap Analysis

Mapping of failed findings to regulatory and industry compliance frameworks. A gap indicates a finding that impacts the specified standard.

FRAMEWORK	GAPS	COMPLIANT	SCORE	GAP DETAILS
CIS FortiGate Benchmark	58	21	27%	ADM-001, ADM-002, ADM-004, ADM-006, SYS-001, SYS-002, SYS-003, SYS-004, SYS-005, SYS-007, SYS-008, SYS-009, SYS-010, POL-001, POL-002, POL-004, POL-005, LOG-001, LOG-002, LOG-004, NTP-002, NTP-003, DNS-002, PWD-001, HA-001, API-001, CRT-001, NET-002, SEC-002, LIP-001, WF-002, WF-003, WF-004, IPS-001, IPS-004, DNSSEC-001, DNSSEC-002, AV-002, AV-003, AV-004, AV-005, SSL-002, SSL-003, APPCTRL-002, APPCTRL-003, FG-001, FG-002, FG-003, TF-001, PCOV-001, PCOV-002, PCOV-003, PCOV-004, PCOV-005, PCOV-006, DOS-001, SDWAN-001, SDWAN-002
ISO 27001	45	7	13%	ADM-001, ADM-002, ADM-004, ADM-006, SYS-001, SYS-002, SYS-003, SYS-004, SYS-007, SYS-008, SYS-009, SYS-010, POL-001, POL-002, POL-004, POL-005, LOG-001, LOG-002, LOG-004, NTP-003, DNS-002, PWD-001, HA-001, API-001, CRT-001, NET-002, SEC-002, LIP-001, WF-002, WF-003, WF-004, IPS-001, IPS-004, DNSSEC-002, AV-002, AV-003, SSL-002, APPCTRL-002, APPCTRL-003, TF-001, PCOV-001, PCOV-006, DOS-001, SDWAN-001, SDWAN-002
PCI-DSS	43	17	28%	ADM-001, ADM-002, ADM-004, ADM-006, SYS-001, SYS-002, SYS-003, SYS-005, SYS-007, SYS-008, SYS-010, POL-001, POL-002, POL-004, POL-005, LOG-001, LOG-002, NTP-002, PWD-001, API-001, SEC-002, LIP-001, WF-002, WF-003, IPS-001, IPS-004, DNSSEC-001, AV-002, AV-003, AV-004, AV-005, SSL-002, SSL-003, APPCTRL-002, FG-001, FG-002, FG-003, PCOV-001, PCOV-002, PCOV-003, PCOV-004, PCOV-005, PCOV-006
CERT-In	20	3	13%	ADM-001, ADM-002, SYS-001, SYS-002, SYS-003, SYS-010, POL-001, POL-002, POL-004, LOG-001, LOG-002, PWD-001, API-001, SEC-002, LIP-001, IPS-001, DNSSEC-002, AV-002, AV-005, TF-001
RBI IT Framework	7	0	0%	ADM-002, ADM-004, SYS-002, POL-001, POL-004, LOG-001, PWD-001
SEBI CSCRF	3	0	0%	ADM-002, POL-001, LOG-001
DPDPA 2023	2	0	0%	ADM-001, PCOV-001