Ultimate GRC Checklist for CISOs & InfoSec Managers

Governance, Risk, and Compliance (GRC) excellence is now a board-level expectation. Use this end-to-end checklist—mapped to ISO 27001:2022, SOC 2, GDPR, India's Digital Personal Data Protection Act ("DPDP Act"), and HIPAA—to benchmark, remediate, and showcase your security program.

How to Use This Checklist

1. **Baseline first:** Execute the "Core Controls" section; these items map to IG1/Level 1 safeguards and satisfy 80% of auditors' initial requests[1][2].
2. **Layer maturity:** Advance through Maturity Levels 2-4 to reach a fully optimized cyber-resilience posture[3][4].
3. **Show evidence:** For every item, attach artifacts (policy docs, SIEM screenshots, scan reports) before declaring "Done."
4. **Report up:** Convert the scorecard at the end into a board-ready slide per CISO reporting best practice[5][6].

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND

The NIST Cybersecurity Framework wheel illustrates five core functions: Identify, Protect, Detect, Respond, and Recover.

Section 1 – Core Controls (Maturity Level 1 “Initial”)

#	Control	Framework Map	Status
1	**Asset Inventory** – Maintain real-time list of endpoints, servers, cloud resources[2]	ISO 27001 8.1; SOC 2 CC1.4	☐
2	**Software Inventory** – Authorize and track all OS / apps; block shadow IT[2]	ISO 27001 8.1; SOC 2 CC1.4	☐
3	**Data Classification Scheme** – Tag PHI, PCI, PII per GDPR Art. 30, HIPAA §164.308[7][8]	GDPR, HIPAA, DPDP	☐
4	**Secure Configuration Baselines** – CIS/benchmarks applied; drift monitored[2]	ISO 27001 8.14; SOC 2 CC5.2	☐
5	**Multi-Factor Authentication everywhere** – Privileged & remote users[9]	ISO 27001 Annex A 5.17; SOC 2 CC6.3	☐
6	**Vulnerability Management** – Authenticated scans every 14 days; SLA-based patching[10]	ISO 27001 8.8; SOC 2 CC7.1	☐
7	**Security Awareness Training** – 100% staff; phishing simulations ≤ 4% fail rate[11]	ISO 27001 6.3; HIPAA §164.308(a)(5)	☐
8	**Incident Response Plan** – 72-hour breach notice workflow for GDPR/DPDP[7]	ISO 27001 5.25; GDPR Art. 33	☐
9	**Logging & SIEM** – Centralize logs; 30-day hot, 365-day cold retention[9][10]	ISO 27001 8.15; SOC 2 CC7.2	☐
10	**Third-Party Risk Register** – Inventory vendors; collect SOC 2/ISO reports annually[12][13]	ISO 27001 5.19; SOC 2 CC3.4	☐

Section 2 – Managed Controls (Maturity Level 2 “Repeatable”)

#	Control	Framework Map	Status
11	**Board-Approved Security Charter** – Defines CISO authority & budget[6]	ISO 27001 5.2, 5.3	☐
12	**Risk Appetite Statement** – Quantified in $$; aligned with ERM[14][15]	ISO 27001 5.4; SOC 2 CC1.2	☐
13	**Formal GRC Tooling / Automation** – Evidence collection & continuous control testing[16][17]	All	☐
14	**Zero-Trust Network Segmentation** – Crown-jewel isolation validated via pen test	ISO 27001 8.9	☐
15	**Data Loss Prevention** – Block outbound PII/PHI exfiltration; alert to SOC[7]	HIPAA, GDPR	☐
16	**Encryption at Rest & in Transit** – AES-256 / TLS 1.3; keys in HSM[7][18]	ISO 27001 8.10; SOC 2 CC6.1	☐
17	**Identity Governance & Lifecycle** – JML tasks auto-provisioned; quarterly UARs[19]	ISO 27001 5.20; SOC 2 CC6.2	☐
18	**Business Continuity & DR Tests** – Prove RTO/RPO; tabletop exec drill 1×/yr[9]	ISO 27001 8.4; SOC 2 CC7.4	☐

19	**Privacy Impact Assessments** – Per system; documented DPIA for GDPR high-risk[20]	GDPR Art. 35; DPDP §10	☐
20	**HIPAA-Specific Controls** – BA Agreements, SRA documentation, audit trails[7]	HIPAA 164 Sub-Parts	☐

A visual representation of the four GRC maturity levels showing a progression from Traditional to Optimal along a winding path.

Section 3 – Advanced Controls (Maturity Level 3 “Defined”)

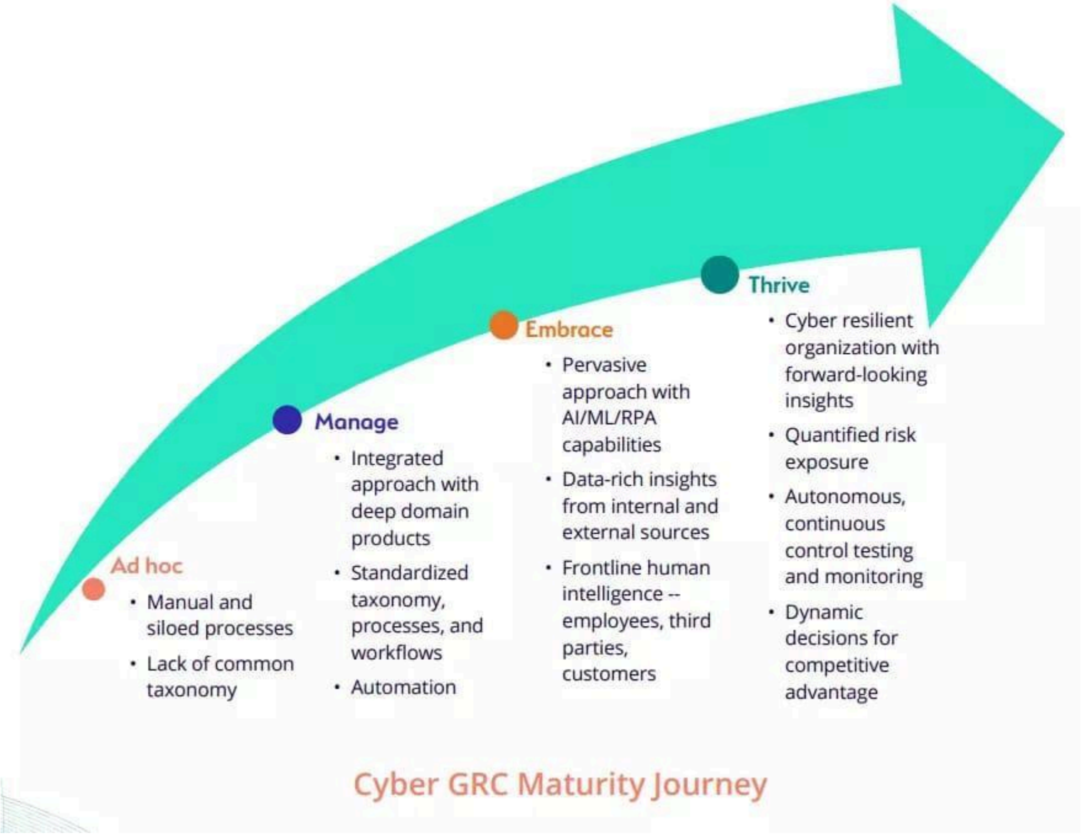
#	Control	Framework Map	Status
21	**Continuous Threat Exposure Mgmt (CTEM)** – Breach-path validation & scoring[21]	ISO 27005; NIST CSF Detect	☐
22	**KPIs & KRIs Dashboard** – MTTD ≤ 4 h, MTTR ≤ 24 h, Unpatched Critical < 2%[10][11]	Board reporting	☐
23	**Supply-Chain Assurance** – SBOM ingestion; monitor exploits (e.g., PCI DSS 4.0 req. 6.4)[22][2]	ISO 27001 5.19	☐
24	**AI/ML Governance** – Model inventory, bias testing, secure-coding SAST[23][22]	ISO 42001 draft; NIST AI RMF	☐
25	**De-Identification & Pseudonymization** – Tokenize live production data[7]	GDPR Art. 25; DPDP Act	☐
26	**Automated Compliance Mapping** – One control → multi-framework evidence[16][24]	All	☐
27	**Security Metrics in OKRs** – Cyber goals tied to revenue, customer trust[25]	Board	☐
28	**Red/Blue/Purple Team Exercises** – 2× /yr; lessons fed into IR playbooks	ISO 27001 8.16	☐

29	**Cloud-Native Security Posture Mgmt** – CSPM policy-as-code; IaC scanning[26]	ISO 27017; SOC 2 CC5.3	☐
30	**Formal Data Retention & Right-to-Erase** – Meet GDPR Art. 17 & DPDP §18[20]	GDPR/DPDP	☐

Section 4 – Optimized Controls (Maturity Level 4 “Managed/Optimizing”)

#	Control	Framework Map	Status
31	**Govern Function Overlay** – Align org cyber-objectives to NIST CSF 2.0 “Govern” outcomes[27][28]	NIST CSF 2.0	☐
32	**Board-Level Risk Quantification** – FAIR or $-based loss exceedance curves[10][25]	ISO 27005	☐
33	**Autonomous Control Validation** – API-driven evidence to auditors in real time[16]	SOC 2 CC3.1	☐
34	**Integrated Privacy & Security Governance** – Unified PDPC/DPDP + HIPAA dashboards[29]	GDPR, DPDP	☐
35	**Predictive Analytics for Risk** – AI models flag trends; feed into quarterly strategy[22][23]	OCEG Level 5	☐
36	**Dynamic Policy as Code** – Controls enforced via CI/CD gates; audited automatically[30]	ISO 27001 8.28	☐

37	**RegTech Watchlist Automation** – Alerts on new laws (e.g., NIS2, DORA)[31][22]	Compliance	☐
38	**Proactive Crisis Communications Plan** – Exec-approved scripts; media training completed[15]	ISO 27001 5.26	☐
39	**Zero-Day Response Playbook** – 24-h patch SLA; threat intel partnerships	ISO 27001 8.12	☐
40	**Sustainability & ESG Alignment** – Map cyber-resilience to ESG Impact metrics[12]	GRI, SASB	☐


Ad hoc
• Manual and siloed processes
• Lack of common taxonomy
Manage
• Integrated approach with deep domain products
• Standardized taxonomy, processes, and workflows
• Automation
Embrace
• Pervasive approach with AI/ML/RPA capabilities
• Data-rich insights from internal and external sources
• Frontline human intelligence -- employees, third parties, customers
Thrive
• Cyber resilient organization with forward-looking insights
• Quantified risk exposure
• Autonomous, continuous control testing and monitoring
• Dynamic decisions for competitive advantage

Cyber GRC Maturity Journey

Cyber GRC maturity journey illustrating four stages from Ad Hoc to Thrive with key characteristics for each stage.

Compliance Framework Cross-Reference

Control Domains	ISO 27001:2022 Clauses/Annex A	SOC 2 TSC	GDPR & DPDP	HIPAA Security Rule
Governance & Leadership	4, 5	CC1	Art. 5-6	164.308(a)(1)
Risk Management	6.1, 8.2-8.3	CC3	Recital 75	164.308(a)(1)(ii)(A)
Asset & Config Mgmt	8.1, 8.9	CC5	Art. 32	164.310
Access Control	5.20, 8.2	CC6	Art. 25 (privacy-by-design)	164.312(a)
Security Operations	8.12-8.16	CC7	Art. 33-34 (breach)	164.308(a)(6)
Incident Response & BCP	5.24-5.26, 8.4	CC7.4	Art. 35-36	164.308(a)(7)
Vendor / Third-Party	5.19	CC3.4	Art. 28	164.308(b)
Privacy & Data Subject Rights	N/A (ISO 27701)	CC2.3	Art. 15-23; DPDP§12-18	164.520

GRC Scorecard

Add your completion % for each section. Aim for ≥ 90% to claim “audit-ready” status.

Section	Completed Items	% Complete
Core Controls	___ /10	___ %
Managed Controls	___ /10	___ %
Advanced Controls	___ /10	___ %
Optimized Controls	___ /10	___ %

Next Steps & Resources

1. **Gap-remediation sprint:** Prioritize unchecked Core items—these map to high-impact vulnerabilities[1][32].
2. **Schedule readiness review:** Engage an external assessor for ISO 27001 Stage 1 or SOC 2 readiness[33][34].
3. **Automate evidence:** Trial a compliance automation platform to slash audit prep time by 82%[16].
4. **Board briefing:** Use the scorecard + KPI dashboard in your next quarterly cyber update[5][6].

Keep this checklist alive—revisit after every significant change and at least quarterly to sustain continuous compliance.

Security is a journey—keep climbing the maturity mountain!

⁂

1. https://www.cisecurity.org/controls/implementation-groups
2. https://www.cisecurity.org/controls/cis-controls-list
3. https://secureframe.com/hub/grc/maturity
4. https://insightassurance.com/understanding-the-grc-maturity-model-a-comprehensive-guide/
5. https://www.hackthebox.com/blog/ciso-board-reporting-template
6. https://www.secureworks.com/resources/wp-a-toolkit-for-cisos
7. https://www.processunity.com/6-security-controls-need-general-data-protection-regulation-gdpr/
8. https://www.akamai.com/glossary/what-is-gdpr
9. https://fudosecurity.com/wp-content/uploads/2024/01/EDITED_CISO-CHECKLISTA-2024_V1-1.pdf
10. https://strobes.co/blog/30-cybersecurity-metrics-kpis/
11. https://www.upguard.com/blog/cybersecurity-metrics
12. https://www.metricstream.com/learn/secure-cloud-strategic-priorities-cyber-risk.html

13. https://www.scrut.io/post/compliance-frameworks
14. https://www.evanta.com/resources/ciso/survey-report/top-3-priorities-for-cisos-in-2025
15. https://www.rmmagazine.com/articles/article/2024/05/02/10-tips-for-developing-an-effective-erm-program
16. https://sprinto.com/blog/compliance-automation-tools/
17. https://www.centraleyes.com/best-compliance-automation-tools/
18. https://www.kiteworks.com/secure-file-transfer/security-governance/
19. https://www.idsalliance.org/blog/six-identity-governance-trends-to-follow-in-2025/
20. https://gdpr.eu
21. https://info.xmcyber.com/ciso-guide-to-reporting-risk-to-the-board
22. https://www.onetrust.com/blog/10-grc-trends/
23. https://www.wwt.com/wwt-research/security-priorities-for-2025
24. https://sprinto.com/blog/compliance-framework/
25. https://www.cyberark.com/resources/blog/5-strategies-for-setting-the-right-cybersecurity-kpis
26. https://kpmg.com/in/en/insights/2025/03/cybersecurity-considerations-2025/government-public-sector.html
27. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
28. https://www.balbix.com/insights/nist-cybersecurity-framework/
29. https://www.kiteworks.com/risk-compliance-glossary/information-security-governance/
30. https://www.logicgate.com/blog/the-5-layers-of-a-mature-grc-program/
31. https://www.forbes.com/councils/forbestechcouncil/2025/03/04/how-cisos-will-navigate-the-threat-landscape-differently-in-2025/
32. https://purplesec.us/learn/security-controls/
33. https://www.vanta.com/collection/grc/preparing-for-a-compliance-audit