Chinmay Dhok

Master Self-Assessment & Accomplishments Record
Role: Senior Information Security Analyst I **Review Period:** November 2025 – August 2026

Executive Summary

Over a 9-month review period (Nov 2025 – Aug 2026), the Information Security function delivered over **100 completed initiatives** across cloud governance, code supply chain protection, regulatory compliance, enterprise deal enablement, and IT SaaS cost optimization.

Key milestones include achieving **ISO 27001:2022 re-certification with zero major non-conformities**, renewing **SOC 2 Type II** compliance with clean reports, auditing and securing **524 GitHub code repositories**, resolving critical endpoint hardware degradation across macOS devices, completing major enterprise TPRM clearances (Global Data Science Retailer, Leading FinTech & Payments Gateway, Major Payment Solutions Provider, Prominent FinTech Unicorn), and automating security operations through self-built AI tools.

Core Metrics Dashboard

Strategic Focus Area	Primary Metric / Target	Organizational Impact
Code Supply Chain Security	524 Repositories Audited & Remediated	Zero active IOCs/malware; 42 repos patched for high-severity Axios vulnerabilities; Litellm package pinning.
Certifications & Compliance	0 Major Non-Conformities	ISO 27001:2022 re-certified; SOC 2 Type II report issued; 100% DPDPA & privacy compliance.
Endpoint & Fleet Governance	90%+ Fleet Stability Achieved	Eliminated 20–30% Mac CPU/battery drain caused by Intune loops; trialed IT Partner & Hexnode.
Identity & SaaS Optimization	267 GWS Accounts & 56 Gemini Seats	Right-sized tiers; purged stale/suspended accounts; zero unmonitored SaaS overhead.
Enterprise TPRM & Sales	100% On-Time Partner Approvals	Unlocked commercial deals with Global Data Science Retailer, Leading FinTech & Payments Gateway, Major Payment Solutions Provider, Prominent FinTech Unicorn, Fortune 500 FMCG Enterprise, Multinational Retail Chain.

Executive Praise & Stakeholder Recognition

> *"Great job to run the compliance process across the org."*
> **— VP of Engineering / CTO (on achieving SOC 2 Type II compliance)**

> *"A huge shout-out to Chinmay for owning the InfoSec questionnaire end-to-end in the recent RFPs/RFIs! Chinmay's turnaround time was lightning fast—every response came back quicker than we could have hoped, which kept the entire conversation moving without a single blocker. You've truly been the backbone of this InfoSec side of the world."*
> **— Sales Leadership (Endorsed with 28 team reactions)**

> *"Absolute Superstar! No reminders, no follow-ups - just flawless execution at lightning speed. Blink, and it's already done."*
>
> **— RFP/RFI Delivery Lead**

> *"Great submission... clear, complete, and exceptionally structured."*
>
> **— Global Organisational Resilience & Internal Investigations Manager (on TPRM submission)**

1. Endpoint Security, Fleet Optimization & MDM Modernization

1.1 Internal Infrastructure & Endpoint Security Audit

- **The "Intune Tax" Discovery:** Identified that severe user complaints regarding 20–30% battery drain, fan noise, and overheating on macOS devices were directly caused by infinite retry loops within the Microsoft Intune Management Extension (IME) agent.
- **Linux Infrastructure Gap:** Uncovered that Linux development machines were entirely unmanaged, creating compliance gaps in SSH key rotation, OS patching, and central visibility.
- **Identity Fragmentation:** Identified a lack of true Single Sign-On (SSO) synchronization between local device logins and Google Workspace credentials.

1.2 Phase 1: Fleet Stabilization & Remediation Execution

- Guided Senior System Administrator to strip out conflicting legacy configurations causing Intune infinite loops.
- Re-architected OS update policy windows to align with local business hours (IST) to prevent background CPU spikes.
- Successfully completed user acceptance testing on internal test devices by January 7, 2026. Following data validation, deployed stabilized policies company-wide, restoring fleet performance.

2. Security Governance, Cloud Architecture & Threat Defense

2.1 Code Supply Chain Protection & Dependency Hardening

- **524 Repository Audit:** Executed an automated, org-wide GitHub audit across 524 code repositories, confirming zero active Indicators of Compromise (IOCs) or malware.
- **Axios Patching:** Identified and remediated critical high-severity vulnerabilities in axios, upgrading 42 affected repositories to version >= 1.8.2.
- **Package Safe-Pinning:** Implemented strict semantic version pinning for critical core packages (including litellm), neutralizing upstream supply-chain injection vectors.
- **CI/CD Security Pipelines:** Integrated AI tools and automated CodeReview security dashboards directly into GitHub Actions CI/CD workflows to block non-compliant PRs before merging.

2.2 GCP Access Governance, PAM & Zero-Trust Architecture

- **Privileged Access Management (PAM):** Engineered and deployed GCP PAM entitlements as Terraform code, establishing scoped read, contribute, and admin tiers with a production guide.
- **Zero-Trust Network Perimeter:** Transitioned legacy VPN entry points to encrypted, audit-logged Tailscale remote access.

- **Secure GCS Provisioning:** Designed production-grade GCS buckets for developer CMS workloads enforcing Uniform Bucket-Level Access (UBLA) and Public Access Prevention (PAP).
- **SCC Findings Triage:** Triaged and resolved 42 critical GCP Security Command Center findings, addressing HAProxy public exposure, over-privileged SAs, and unrotated keys.

2.3 Incident Response, VAPT & Monitoring Enhancements

- **Offensive VAPT:** Executed internal security testing across web applications, iOS/Android SDKs, and in-store Ad Servers, resolving CORS misconfigurations, rate limiting gaps, and business logic flaws.
- **Threat Neutralization:** Executed org-wide Internal Vulnerability Scanners for CVE-2026-45321 (TanStack) and remediated a cryptomining compromise on a test-framework project.
- **Real-Time Observability:** Built automated Cloud SQL memory/CPU spike alerts and continuous health monitoring for the Core Backend Architecture.

3. Compliance Frameworks, Certifications & Policy Audits

Standard	Result	Strategic Focus & Artifacts
ISO 27001:2022	Certified (0 Major NCs)	Stage-2 Surveillance Audit completed June 2026.
SOC 2 Type II	Report Issued (Clean)	Full evaluation period verified with clean opinion.
GDPR / CCPA	Satisfactory Rating	Audited transfers, cookie consent, DSAR SLAs, retention.
DPDPA (India)	Fully Compliant	Published website disclosures and opt-in forms.
Policy Governance	54 Policies Modernized	Utilized LLM + manual review to purge legacy clauses.

4. Enterprise TPRM, RFPs & Commercial Deal Enablement

4.1 Global Data Science Retailer Enterprise TPRM Clearance

- **High-Availability Architecture:** Evidenced a 99.9% Uptime SLA backed by multi-region, geo-redundant GKE clusters across North America and the EU. Documented failover mechanics utilizing GCP Load Balancing, Cloud Armor WAF, and DNS routing.
- **Data Residency & Controls:** Detailed primary hosting in us-central1 with European options. Demonstrated SHA256 irreversible hashing for PII, 13-month campaign data retention, and 7-year financial record retention.
- **Trust Verification:** Delivered audited SOC 2, ISO, penetration test, and security artifacts via the Security Trust Vault.

4.2 Enterprise Partner Onboarding & Vendor Management

- **Leading FinTech & Payments Gateway BGV Compliance:** Evaluated background verification vendors to satisfy enterprise requirements, onboarding Background Verification Vendor as a cost-effective, compliant solution.
- **Major Payment Solutions Provider Clearance:** Resolved complex DPA technical queries, updated network topologies, and secured risk committee sign-off.
- **Prominent FinTech Unicorn Risk Assessment:** Authored response matrices and evidence packets covering encryption, IR, network isolation, and DR protocols.

- **RFP Acceleration:** Authored security attestations that unblocked enterprise deals for Fortune 500 FMCG Enterprise, Multinational Retail Chain, Leading FinTech & Payments Gateway, and Global Telecommunications Provider.

5. Enterprise IT Operations & SaaS Cost Optimization

- **Google Workspace (GWS) Migration:** Led a domain-wide migration and license restructuring across 267 Google Workspace user accounts, right-sizing operational seats to lower cost tiers.
- **Account Sanitization:** Permanently purged suspended, offboarded, and unassigned licenses, eliminating recurring subscription waste.
- **Enterprise Gemini AI Seat Optimization:** Audited usage metrics across 56 licenses. Reallocated dormant seats directly to active engineering and product teams, maximizing tool ROI and eliminating idle licensing costs.

6. Email, Brand Trust & Network Security

- **Gmail BIMI & VMC Rollout:** Secured DigiCert VMC approval, aligned DMARC policies (p=reject), and deployed SVG/PEM assets to S3, establishing verified blue checkmark domain authentication.
- **Anti-Phishing Defense:** Neutralized an active invoice-fraud phishing campaign targeting Finance, identifying typosquat domains and updating Workspace blocked-sender rules.
- **Ad Server & Office Network Hardening:** Hardened office and in-store networks with gateway traffic shaping (30/2 Mbps), IDS/IPS controls, DHCP IP-MAC binding for 190 laptops, and AP alert policies.
- **Security Automation:** Developed a Google Apps Script mail-merge system, Chrome extension security auditor (~194 users reviewed), and Zoho ticketing automation for daily network health checks.

7. Strategic Focus & Roadmap (Upcoming Initiatives)

- **VAPT Expansion:** Conducting security testing on Partner Portal UI (Next.js / Supabase).
- **AI Tooling V2:** Deploying Security RFP Gemini App V2 and automated phishing simulation programs via Google Apps Script.
- **GCP Threat Detection Buildout:** Expanding logging and scanning across Cloud Run, Container Registry, Cloud DNS, Artifact Guard, and Notebook Security Scanner.
- **Advanced Access Controls:** Implementing Context-Aware Access, Google Workspace DLP policies, and Mobile Device Management (MDM) for iOS/Android.
- **Cyber Insurance:** Finalizing feature enablement and eligibility assessment for Enterprise Cyber Insurance coverage.