CSAT Partner Engagement Playbook

# Introduction

The Compliance & Security Assurance Team (CSAT) strengthens the organization’s compliance and security posture through consistent, meaningful engagement with business partners. This playbook defines how CSAT will interact with stakeholders, ensuring that compliance and security activities are proactive, transparent, and collaborative.

# Engagement Principles

• Partnering, not policing – focus on collaboration over enforcement

• Early engagement – involve CSAT at project inception, not just during audits

• Transparency – provide visibility into risks, metrics, and compliance status

• Accountability – define clear ownership for actions and follow-ups

# Core Engagement Activities

1. Regular Communication

• Quarterly business unit reviews of compliance health and risks

• Bi-weekly office hours for ad hoc partner questions

• Monthly dashboard updates to track progress and issues

2. Project & Initiative Involvement

• Intake reviews for all new projects and vendor onboardings

• Participation in project kickoffs to highlight compliance/security requirements early

• Continuous advisory support for policy and control interpretation

3. Training & Awareness

• Targeted workshops (e.g., PCI scope management, access review automation)

• Creation of lightweight playbooks and quick guides for recurring compliance tasks

• CSAT onboarding sessions for new leaders and teams

4. Feedback & Relationship Building

• Quarterly feedback survey to assess partner satisfaction and effectiveness

• Post-audit retrospectives to capture lessons learned

• Recognition of teams demonstrating strong compliance practices

5. Measurement & Metrics

• Engagement Coverage: % of business units engaged per quarter

• Partner Satisfaction: Survey results and anecdotal feedback

• Compliance Outcomes: Fewer audit findings, faster remediation timelines

# Engagement Cadence

• Weekly: Office hours, intake triage, partner responses

• Monthly: Dashboards and compliance check-ins with stakeholders

• Quarterly: Business unit reviews and partner surveys

• Annually: Enterprise-wide compliance review and executive summary

# Roles & Responsibilities

• CSAT Lead: Oversees engagement strategy, reporting, and escalations

• Partner Liaison: Manages partner meetings, communications, and surveys

• Compliance Analyst: Provides audit readiness insights and remediation tracking

• Security Engineer: Advises on technical remediation and monitoring tools

• Product Owners: Engage proactively with CSAT and address compliance tasks

# Reporting & Continuous Improvement

• Quarterly Executive Dashboard: Tracks engagement coverage, risk trends, and outcomes

• Continuous Feedback Loop: Incorporate survey results and lessons learned into process improvements

• Automation Opportunities: Identify manual processes suitable for automation to improve partner experience

**CSAT Responsibilities**

**1. Compliance & Audit Readiness**

• Align policies and controls with PCI and other regulatory standards

• Support audits by preparing evidence, coordinating with stakeholders, and closing findings

• Maintain continuous audit readiness with up-to-date documentation and control evidence

**2. Security Assurance Health**

• Monitor and report on patching, SIEM, FIM, DR, anti-malware, and vulnerability scans

• Assist with attestations (e.g., quarterly access reviews, control validations in eGRC)

• Track audit/security findings and ensure timely remediation

• Provide leadership with visibility into recurring issues and risk posture trends

**3. Patch Oversight**

• Deliver monthly patch compliance dashboards with ≥98% accuracy

• Review and approve/deny patch exceptions within 3 business days

• Escalate overdue critical patches within 1 business day; notify leadership of exposures within 48 hours

• Provide patch-related audit evidence within 48 hours of request

• Conduct quarterly patch health reviews with BUs and ensure timely responses to inquiries

**4. Partner Engagement**

• Conduct quarterly BU check-ins for compliance and risk posture reviews

• Deliver targeted training and awareness sessions (e.g., PCI scope, access reviews)

• Collect partner feedback via surveys and retrospectives; recognize strong compliance performance

**5. Continuous Improvement**

• Automate manual workflows for compliance, patch oversight, and reporting where possible

• Improve SLA compliance and partner experience through process optimization

• Provide executives with dashboards and RAG indicators for rapid decision-making