



Risk Assessment and Treatment Process

Control Page

ATTRIBUTE	DETAIL
Document Title	Risk Assessment and Treatment Process
Document ID	OG-RATP-001
Version	1.1
Effective Date	November 2, 2025
Next Review Date	November 2, 2026 (Annual)
Policy Owner	Chief Security & Compliance Officer (CSCO)
Approved By	Chief Executive Officer (CEO)
Classification	Confidential – Internal Use Only
Applicability	All personnel involved in managing, operating, or supporting the Cardholder Data Environment (CDE)



Compliance Frameworks	PCI DSS v4.0, ISO/IEC 27001:2022, NIST SP 800-30, GDPR (where applicable)
Distribution List	Engineering, IT, DevOps, Security, Internal Audit, Executive Leadership

Approvals

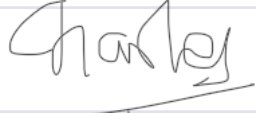
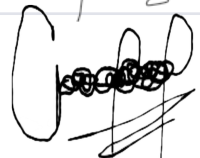
NAME	POSITION	SIGNATURE	DATE
Oleksii Bondarenko	Chief Security & Compliance Officer		1 November 2025
Charles Odhiambo	Technical Lead		1 November 2025
Kevin Kegera	Chief Commercial Officer		1 November 2025
Preston Obadan	Chief Executive Officer		1 November 2025



Table of Contents

1. Introduction

- 1.1 Purpose
- 1.2 Scope
- 1.3 Objectives
- 1.4 Regulatory and Standards Alignment
- 1.5 Definitions and Acronyms

2. Risk Assessment Framework

- 2.1 Foundational Principles
- 2.2 Risk Identification
 - 2.2.1 Asset Inventory and CDE Boundary Mapping
 - 2.2.2 Threat Intelligence Integration
 - 2.2.3 Vulnerability Discovery Sources
- 2.3 Risk Analysis
 - 2.3.1 Qualitative Risk Scoring Model
 - 2.3.2 Impact Criteria
 - 2.3.3 Likelihood Criteria
- 2.4 Risk Evaluation
 - 2.4.1 Risk Appetite Statement
 - 2.4.2 Risk Categorization

3. Risk Treatment Methodology

- 3.1 Treatment Strategy Selection
- 3.2 Control Design and Selection
 - 3.2.1 Control Sourcing (Preventive, Detective, Corrective)
 - 3.2.2 Mapping to PCI DSS and ISO 27001
- 3.3 Implementation Workflow
 - 3.3.1 Integration with Change Management
 - 3.3.2 Testing and Validation
- 3.4 Residual Risk Management
 - 3.4.1 Residual Risk Recalculation
 - 3.4.2 Formal Risk Acceptance Protocol

4. Roles and Responsibilities

- 4.1 Chief Security & Compliance Officer (CSCO)
- 4.2 Engineering and DevOps Leadership
- 4.3 Security Operations Center (SOC)
- 4.4 Internal Audit
- 4.5 Executive Leadership (CEO, CCO)
- 4.6 Third-Party Vendors

5. Documentation, Recordkeeping, and Auditability

- 5.1 Risk Register Structure and Governance
- 5.2 Evidence Management for Controls
- 5.3 Audit Trail and Version Control
- 5.4 Integration with GRC Platform



6. Monitoring, Review, and Continuous Improvement

- 6.1 Continuous Risk Monitoring
- 6.2 Trigger Events for Reassessment
- 6.3 Performance Measurement and KPIs
- 6.4 Lessons Learned and Process Optimization

7. Appendices

- 7.1 Risk Scoring Matrix (5×5 Model)
- 7.2 Sample Risk Register Template (Enhanced Fields)
- 7.3 Risk Treatment Decision Workflow Diagram
- 7.4 Risk Acceptance Request Form (Template)



1. Introduction

1.1 Purpose

This document establishes Orchestrate Global's enterprise-wide Risk Assessment and Treatment Process (RATP)—a systematic, repeatable, and auditable methodology for proactively identifying, analyzing, evaluating, and treating risks that could compromise the confidentiality, integrity, or availability of cardholder data. The RATP serves as the cornerstone of the organization's Information Security Management System (ISMS) and is integral to maintaining compliance with PCI DSS and other relevant regulatory frameworks.

1.2 Scope

The RATP applies to all components of the Cardholder Data Environment (CDE), including but not limited to:

- Physical and virtual servers hosting payment applications
- Network segments that transmit or route cardholder data
- Databases storing primary account numbers (PANs), cardholder names, service codes, or expiration dates
- Endpoints (laptops, mobile devices) used to access CDE systems
- Third-party service providers with CDE connectivity (e.g., payment gateways, hosting providers)
- Development, staging, and testing environments that replicate CDE functionality

The scope explicitly excludes non-CDE systems unless they are in-scope via segmentation validation or shared dependencies (e.g., authentication directory).

1.3 Objectives

- Ensure risks to the CDE are identified before they result in compromise
- Provide a consistent, defensible methodology for risk quantification



- Enable informed, risk-based decision-making by leadership
- Support continuous compliance with PCI DSS Requirement 12.3 and related controls
- Foster a culture of proactive risk ownership across technical and business units

1.4 Regulatory and Standards Alignment

This process is explicitly designed to satisfy:

- PCI DSS v4.0: Requirements 6.2 (vulnerability management), 12.1 (risk assessment policy), 12.3 (formal risk assessment process), and 12.10.2 (risk treatment documentation)
- ISO/IEC 27001:2022: Clauses 6.1.2 (Information security risk assessment) and 6.1.3 (Information security risk treatment)
- NIST SP 800-30: Guide for Conducting Risk Assessments
- GDPR Article 32: Security of processing (where EU cardholder data is involved)

1.5 Definitions and Acronyms

- CDE: Cardholder Data Environment — the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.
- Inherent Risk: Risk level before any controls are applied.
- Residual Risk: Risk level remaining after controls are implemented.
- Risk Appetite: The level of risk Orchestrate Global is willing to accept in pursuit of its strategic objectives (defined annually by the Board).
- GRC: Governance, Risk, and Compliance platform used for centralized policy and risk management.
- SoA: Statement of Applicability — document mapping controls to compliance requirements.

2. Risk Assessment Framework

2.1 Foundational Principles

The RATP is grounded in three core principles:

1. Proactivity: Risks are assessed continuously, not reactively.



2. Proportionality: Assessment depth aligns with asset criticality.
3. Accountability: Every risk has a designated owner responsible for treatment.

2.2 Risk Identification

Risks are systematically identified through multiple concurrent channels:

2.2.1 Asset Inventory & CDE Boundary Mapping

A dynamic, automated inventory (maintained via CMDB) identifies all assets with CDE relevance. Network segmentation diagrams are validated quarterly to ensure accurate boundary definition.

2.2.2 Threat Intelligence Integration

Internal SIEM and external threat feeds (e.g., FS-ISAC, MITRE ATT&CK) inform emerging threat scenarios relevant to payment systems (e.g., supply chain attacks, zero-day exploits in payment SDKs).

2.2.3 Vulnerability Discovery Sources

- Automated scans (authenticated/unauthenticated)
- Penetration tests (internal/external, biannually)
- Code static/dynamic analysis (SAST/DAST)
- Bug bounty and red team findings
- Vendor security advisories

All findings are triaged and entered into the Risk Register within 48 hours.

2.3 Risk Analysis

2.3.1 Qualitative Risk Scoring Model

A 5x5 matrix (see Appendix 7.1) evaluates Likelihood (1–5) and Impact (1–5), producing a numeric Risk Score (1–25).

2.3.2 Impact Criteria



Impact is assessed across three dimensions:

- Confidentiality: Unauthorized disclosure of PANs or authentication data
 - Integrity: Manipulation of transaction data or payment logs
 - Availability: Disruption of payment processing
- Each dimension is scored; the highest score determines overall impact.

2.3.3 Likelihood Criteria

Based on:

- Threat actor capability and motivation
- Existing compensating controls
- Historical incident data
- System exposure (internet-facing vs. internal)

2.4 Risk Evaluation

2.4.1 Risk Appetite Statement

Orchestrate Global's current risk appetite (approved November 2025) states:

"No High or Critical residual risks will be accepted in the CDE without explicit CEO approval.
Medium risks must be treated within 90 days."

2.4.2 Risk Categorization

RISK SCORE	CATEGORY	REQUIRED ACTION
16–25	Critical/High	Immediate escalation; treatment within 30 days
9–15	Medium	Treatment plan within 60 days
1–8	Low	Monitor or accept with documentation



3. Risk Treatment Methodology

3.1 Treatment Strategy Selection

For each risk exceeding appetite, the following options are evaluated:

- Avoid: Discontinue the risky activity (e.g., stop storing PANs if not required).
- Mitigate: Apply technical or administrative controls.
- Transfer: Contractual indemnification or cyber insurance (limited to financial impact only).
- Accept: Only permitted for residual risk with executive sign-off.

3.2 Control Design and Selection

3.2.1 Control Sourcing

Controls are selected from three categories:

- Preventive: Firewalls, encryption, access controls
- Detective: IDS/IPS, log monitoring, anomaly detection
- Corrective: Incident response playbooks, backups, patch rollback

3.2.2 Mapping to PCI DSS and ISO 27001

All selected controls are mapped to:

- Specific PCI DSS requirements (e.g., Requirement 3.4 → PAN truncation)

ISO 27001 Annex A controls (e.g., A.8.23 → Information deletion)

- This mapping is maintained in the SoA.

3.3 Implementation Workflow

3.3.1 Integration with Change Management

All risk treatment actions that modify systems or processes must follow the Secure Change Management Policy, including:



- Peer review
- Security impact analysis
- Backout plan

3.3.2 Testing and Validation

Controls are validated through:

- Automated compliance checks (e.g., CIS benchmarks)
- Manual verification by SOC
- Re-scanning to confirm vulnerability closure

3.4 Residual Risk Management

3.4.1 Residual Risk Recalculation

After control implementation, the risk is rescored. If >8, it remains in active tracking.

3.4.2 Formal Risk Acceptance Protocol

High residual risks require:

- Completion of Risk Acceptance Request Form (Appendix 7.4)
- CSCO attestation of due diligence
- CEO signature
- Board-level disclosure

4. Roles and Responsibilities

4.1 Chief Security & Compliance Officer (CSCO)

- Overall ownership of RATP
- Chair of ISSC
- Final authority on risk scoring disputes
- Reports risk posture to Board quarterly

4.2 Engineering & DevOps Leadership



- Ensure risk identification during SDLC
- Implement and test controls
- Maintain asset inventory accuracy

4.3 Security Operations Center (SOC)

- Monitor for risk indicators
- Validate control effectiveness
- Escalate emerging threats

4.4 Internal Audit

- Independent validation of RATP execution
- Test sample of risk treatments annually
- Report gaps to Audit Committee

4.5 Executive Leadership

- Approve risk appetite
- Allocate budget for mitigation
- Accept residual risk at enterprise level

4.6 Third-Party Vendors

- Participate in joint risk assessments
- Provide evidence of controls (e.g., SOC 2 reports)
- Remediate findings per SLA

5. Documentation, Recordkeeping, and Auditability

5.1 Risk Register Structure

Hosted in GRC platform with fields:

Risk ID, Description, Asset(s), Threat, Vulnerability, Inherent Score, Treatment Plan, Owner, Due Date, Control ID, Residual Score, Status, Approval Evidence.

5.2 Evidence Management



All control implementations must include:

- Screenshots/configs
- Test results
- Training records (for procedural controls)
Stored in an encrypted repository with SHA-256 hashing.

5.3 Audit Trail

All actions logged with immutable timestamp, user ID, and change reason. Retained for 7 years.

5.4 GRC Integration

Automated workflows trigger:

- Treatment due date reminders
- Escalations for overdue items
- Reporting to ISSC dashboard

6. Monitoring, Review, and Continuous Improvement

6.1 Continuous Monitoring

- Real-time SIEM correlation rules for CDE anomalies
- Weekly vulnerability scan comparisons
- Monthly threat hunting exercises

6.2 Trigger Events

Mandatory reassessment upon:

- CDE boundary changes
- New payment method integration
- PCI DSS version update
- Breach or near-miss incident

6.3 KPIs



- % High risks closed within SLA
- Mean time to treatment (MTTT)
- Control failure rate
- Audit findings per 100 risks

6.4 Process Optimization

Post-implementation reviews feed into annual RATP updates. Lessons from incidents are codified into prevention playbooks.

7. Appendices

7.1 Risk Scoring Matrix (5x5)

LIKELIHOOD/IMPACT	1(MINIMAL)	2(MINOR)	3(MODERATE)	4(MAJOR)	5(CATASTROPHIC)
5 (Almost Certain)	5	10	15	20	25
4 (Likely)	4	8	12	16	20
3 (Possible)	3	6	9	12	15
2 (Unlikely)	2	4	6	8	10
1 (Rare)	1	2	3	4	5

Thresholds:

- Low: 1–8
- Medium: 9–15
- High: 16–25



7.2 Sample Risk Register Template

(Includes fields for CDE asset tag, PCI DSS requirement reference, treatment cost estimate, and compensating control flag)

7.3 Risk Treatment Decision Workflow

Visual flowchart showing decision gates: Identify → Analyze → Evaluate → Select Treatment → Approve → Implement → Validate → Close or Accept.

7.4 Risk Acceptance Request Form

Structured template requiring: business justification, cost-benefit analysis, mitigation alternatives considered, and executive attestation.

Document End