CC1 — Control Environment

Entity Name	[Company Name]
Audit Period	[Start Date – End Date]
Prepared By	[Name / Title]
Approved By	[Executive Name / Title]
Last Updated	[Date]

Trust Services Criteria: CC1.1 – CC1.5 (COSO Principle 1–5)

Overview

CC1 addresses the organization's commitment to integrity and ethical values, board oversight, organizational structure, commitment to competence, and accountability. This section documents both the technical controls embedded in the system that enforce control environment principles and the organizational policies, processes, and activities required for SOC 2 compliance.

The system implements role-based access controls with a 6-level hierarchy, comprehensive audit logging of all security-relevant actions, separation of duties through structural safeguards, and mandatory MFA policies for privileged roles. Organizational controls — including the Code of Conduct, board oversight processes, training programs, and accountability frameworks — are templated below for completion.

CC1.1 — Integrity and Ethical Values

COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

Control Objectives

The organization establishes standards of conduct, communicates them to personnel, and enforces adherence through disciplinary measures. Technical controls support integrity by preventing unauthorized actions, maintaining audit trails, and enforcing security policies consistently across all users.

Implemented Controls

Comprehensive Audit Trail for Accountability

The system captures 26 audit event types across 8 categories, creating an immutable record of all security-relevant actions:

CATEGORY	EVENTS	INTEGRITY PURPOSE
Authentication	LOGIN_SUCCESS, LOGIN_FAILED, LOGIN_LOCKED, LOGOUT	Track all access attempts
Password	PASSWORD_CHANGED, PASSWORD_RESET_REQUESTED, PASSWORD_RESET_COMPLETED, PASSWORD_REUSE_ATTEMPTED	Enforce credential policies
User Management	USER_CREATED, USER_UPDATED, USER_DEACTIVATED, USER_REACTIVATED, USER_DELETED	Track identity lifecycle
MFA	MFA_ENABLED, MFA_DISABLED, MFA_VERIFIED, MFA_FAILED, MFA_ADMIN_OVERRIDE	Monitor security control changes
Role Changes	USER_ASSIGNED_TO_ORG, USER_ROLE_CHANGED	Track privilege modifications

Each event records: `userId`, `ipAddress`, `userAgent`, `organizationId`, and event-specific metadata. Audit logs are immutable (append-only) with no UPDATE or DELETE operations via the application.

> **EVIDENCE** The logging system documents 26 audit event types with immutable, append-only storage. All security-relevant actions are captured with actor attribution, enabling accountability and integrity monitoring. Show Me

User Enumeration Prevention

The authentication system prevents information disclosure that could be exploited:

- Generic "Invalid credentials" returned for all login failure types (user not found, wrong password, account inactive)
- Password reset returns success for non-existent emails (prevents email enumeration)
- Actual failure reasons recorded in audit logs for internal investigation only

> **EVIDENCE** The authentication system implements consistent error responses across all failure modes, preventing information leakage while maintaining detailed internal audit records for legitimate investigations. Show Me

Self-Serving Action Prevention

The RBAC system implements structural controls that prevent self-serving behavior:

CONTROL	IMPLEMENTATION
Self-deletion prevention	Users cannot delete their own account
Self-elevation block	Role hierarchy check prevents granting self higher roles
Last SuperAdmin protection	System prevents deletion of the last SuperAdmin account
Admin override audit	MFA_ADMIN_OVERRIDE requires mandatory reason and generates CRITICAL alert

> **EVIDENCE** The RBAC system enforces self-deletion prevention, self-elevation blocking, and last-SuperAdmin protection — structural safeguards that prevent individuals from circumventing controls for personal benefit. Show Me

Sensitive Data Sanitization

The logging system automatically redacts sensitive information from logs, enforcing data handling integrity:

- 46 sensitive field patterns redacted (passwords, tokens, PII, financial data)
- URL parameters sanitized (code, token, secret, api_key, authorization)
- `@SkipBodyLogging()` decorator applied to credential-handling endpoints
- Bodies exceeding size limits are skipped entirely

> **EVIDENCE** The logging system implements 46 sensitive field patterns for automatic redaction and URL parameter sanitization, demonstrating a commitment to responsible data handling as part of the organization's integrity posture. Show Me

Organizational & Process Controls

1. Policies & Documents

DOCUMENT	PURPOSE	OWNER	REVIEW CADENCE
[Code of Conduct — maintained by [HR / Legal], reviewed Annually]	Establishes the organization's standards of behavior, ethical expectations, and commitment to integrity for all employees, contractors, and third parties	[General Counsel / CHRO]	Annual
[Disciplinary Policy — maintained by [HR], reviewed Annually]	Defines consequences for violations of the Code of Conduct and organizational policies, including progressive discipline procedures	[HR Director / General Counsel]	Annual
[Background Check Policy — maintained by [HR], reviewed Annually]	Specifies pre-employment screening requirements including criminal background checks, employment verification, and reference checks	[HR Director]	Annual
[Ethics Hotline / Reporting Policy — maintained by [Legal / Compliance], reviewed Annually]	Establishes anonymous and confidential channels for reporting ethical concerns, fraud, and policy violations with non-retaliation protections	[General Counsel / Compliance Officer]	Annual
[Acceptable Use Policy — maintained by [IT / Security], reviewed Annually]	Defines acceptable use of organizational information systems, data, and resources	[CISO / IT Director]	Annual

2. Control Activities

ACTIVITY	FREQUENCY	RESPONSIBLE PARTY	OUTPUT/DELIVERABLE
Code of Conduct annual acknowledgement	Annual	[HR / Compliance]	Signed acknowledgement records for all personnel
Background checks for new hires	Per-event (pre-hire)	[HR]	Completed background check reports
Ethics hotline monitoring and triage	Continuous	[Ethics Committee / Legal]	Intake log and investigation records
Disciplinary action tracking	Per-event	[HR / Management]	Disciplinary action records

ACTIVITY	FREQUENCY	RESPONSIBLE PARTY	OUTPUT/DELIVERABLE
Annual ethics and integrity training	Annual	[HR / Compliance]	Training completion records
Vendor/contractor Code of Conduct acknowledgement	Per-event (onboarding)	[Procurement / Legal]	Signed contractor acknowledgements

3. Monitoring & Enforcement

- **Monitoring method:** [HR / Compliance] tracks Code of Conduct acknowledgement completion rates with target of 100% within [30 days] of distribution. Ethics hotline reports are reviewed by [Ethics Committee] within [5 business days] of submission. Audit logs provide continuous monitoring of actions that may indicate integrity violations
- **Escalation procedures:** Ethics complaints are triaged by [Ethics Committee / General Counsel]. Substantiated violations are escalated per the Disciplinary Policy. Violations involving management are escalated to [Board / Audit Committee]. CRITICAL audit alerts (e.g., MFA_ADMIN_OVERRIDE) are escalated to [CISO] within [4 hours]
- **Consequence of non-compliance:** Failure to acknowledge the Code of Conduct within the required period results in access suspension pending acknowledgement. Substantiated ethics violations result in progressive discipline up to and including termination per the Disciplinary Policy

4. Key Artifacts for Auditors

- [ ] Code of Conduct document (current version)
- [ ] Signed Code of Conduct acknowledgements for all employees during the audit period
- [ ] Background check completion records for all new hires during the audit period
- [ ] Ethics hotline / reporting channel documentation and intake logs (anonymized)
- [ ] Disciplinary action records for the audit period (anonymized)
- [ ] Annual ethics and integrity training materials and completion records

---

CC1.2 — Board Oversight

COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control Objectives

The board of directors (or equivalent oversight body) maintains independence from management, meets with sufficient frequency, and exercises active oversight of the organization's internal control system including security, availability, and compliance.

Implemented Controls

RBAC-Scoped Oversight Access

The system provides role-differentiated access to audit and monitoring data that supports oversight activities:

ROLE	AUDIT LOG ACCESS	ALERT ACCESS	USER MANAGEMENT
SuperAdmin	All audit logs across all organizations	Full alert access and configuration	Full user lifecycle management
Admin	Organization-scoped audit logs	View and acknowledge alerts	Organization-scoped user management
Other roles	No access	No access	No access

This ensures oversight bodies can access comprehensive control effectiveness data while maintaining appropriate access boundaries.

> **EVIDENCE** The RBAC system provides SuperAdmin-level access to all audit logs, alerts, and user management across organizations, enabling board-designated oversight personnel to review control effectiveness across the entire entity. Show Me

Automated Alerting for Oversight

The alerting system automatically surfaces CRITICAL and HIGH events that warrant oversight attention:

ALERT SEVERITY	EXAMPLE EVENTS	OVERSIGHT RELEVANCE
CRITICAL	MFA_ADMIN_OVERRIDE	Administrative override of security controls
HIGH	LOGIN_LOCKED, MFA_DISABLED, USER_DELETED	Potential attack, control removal, data destruction
HIGH	INSTANCE_HEALTH_THRESHOLD, DATABASE_HEALTH_THRESHOLD	Infrastructure availability issues

EVIDENCE The alerting system classifies 11 event types by severity, automatically surfacing CRITICAL and HIGH events that require oversight attention — providing the board with timely visibility into significant control events. Show Me

Organizational & Process Controls

1. Policies & Documents

DOCUMENT	PURPOSE	OWNER	REVIEW CADENCE
[Board / Oversight Committee Charter — maintained by [Board Secretary / Legal], reviewed Annually]	Defines the board's composition, independence requirements, responsibilities for internal control oversight, and meeting cadence	[Board Chair / General Counsel]	Annual
[Audit Committee Charter — maintained by [Board Secretary], reviewed Annually]	Establishes the audit committee's authority, scope, and responsibilities for overseeing financial reporting, compliance, and internal controls	[Audit Committee Chair]	Annual
[Board Independence Policy — maintained by [Legal / Governance], reviewed Annually]	Specifies independence criteria for board members, conflict of interest disclosures, and recusal procedures	[General Counsel / Board Secretary]	Annual
[Control Effectiveness Review Report — maintained by [Internal Audit / CISO], reviewed Quarterly]	Summarizes control design and operating effectiveness for board review, including deficiency status and remediation progress	[CISO / Internal Audit Director]	Quarterly

2. Control Activities

ACTIVITY	FREQUENCY	RESPONSIBLE PARTY	OUTPUT/DELIVERABLE
Board / oversight committee meeting	[Quarterly / Monthly]	[Board Chair / Committee Chair]	Meeting minutes documenting oversight review
Control effectiveness presentation to board	Quarterly	[CISO / Internal Audit Director]	Control effectiveness report and presentation materials

ACTIVITY	FREQUENCY	RESPONSIBLE PARTY	OUTPUT/DELIVERABLE
Annual independence assessment	Annual	[Board Secretary / General Counsel]	Independence certification for each board member
Conflict of interest disclosure collection	Annual	[Board Secretary / Legal]	Signed conflict of interest disclosures
External audit results review	Annual	[Audit Committee]	Minutes documenting review of external audit findings
Information security program review	Annual	[Board / CISO]	Board resolution acknowledging IS program review

3. Monitoring & Enforcement

- **Monitoring method:** [Board Secretary] tracks meeting attendance, quorum requirements, and action item completion. [CISO / Internal Audit] prepares quarterly control effectiveness reports for board review. Board members receive automated alert summaries for CRITICAL events
- **Escalation procedures:** Significant control deficiencies identified between meetings are communicated to [Board Chair / Audit Committee Chair] within [5 business days]. Emergency sessions may be convened for material control failures
- **Consequence of non-compliance:** Board members who fail to meet independence requirements or disclose conflicts of interest are subject to recusal or removal per [Board Independence Policy]. Failure to convene required meetings is documented and reported to [regulators / stakeholders] as applicable

4. Key Artifacts for Auditors

- ☐ Board / Oversight Committee Charter (current version)
- ☐ Board meeting minutes from meetings during the audit period showing internal control oversight
- ☐ Board member independence certifications
- ☐ Conflict of interest disclosures for all board members
- ☐ Control effectiveness reports presented to the board during the audit period
- ☐ Audit Committee meeting minutes (if separate from board)
- ☐ Evidence of board review of external audit results

CC1.3 — Organizational Structure and Authorities

COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control Objectives

The organization maintains a clearly defined organizational structure with documented reporting lines, delegated authorities, and security responsibilities assigned at each level. Role definitions are enforced technically and organizationally.

Implemented Controls

6-Level Role Hierarchy with Defined Authorities

The RBAC system implements a structured authority model with clearly differentiated access levels:

ROLE	PRIORITY	AUTHORITY SCOPE
SuperAdmin	200	Full system access across all organizations — user management, configuration, security overrides
Admin	100	Full access within assigned organizations — user management, audit review, alert acknowledgement
Consultant	75	Manage projects and customers within assigned organizations
Leadership	75	Leadership functions within assigned organizations
Customer	50	View and respond to questionnaires within assigned organizations
Unapproved	0	Pending approval — minimal access (default for new registrations)

Role hierarchy is enforced at every request via the guard pipeline: `JwtAuthGuard → RbacGuard`.

> **EVIDENCE** The RBAC system implements a 6-level role hierarchy with numeric priorities (0–200), enforced at every request via the NestJS guard pipeline. Each role has clearly defined authority scope with organization-level scoping. Show Me

Multi-Tenant Organization Scoping

The system supports multi-tenant organization isolation that maps to organizational structure:

- Users can belong to multiple organizations with one role per organization
- Organization context embedded in JWT tokens for request-level enforcement
- Admin visibility scoped to organizations where they hold the Admin role
- SuperAdmins see across all organizations (entity-wide oversight)

EVIDENCE The RBAC system enforces organization-scoped data visibility with unique constraints (`[userId, organizationId]`) and JWT-embedded organization context, structurally mapping authorities to organizational boundaries. Show Me

Core vs. Application Module Separation

The architecture separates system-level security modules from business-specific modules:

LAYER	MODULES	RESPONSIBILITY
Core	auth, rbac, mfa, audit, alerting, encryption, email, invitation, settings, system, instance-health, database-health, key-rotation, retention, scheduler, logger, prisma, ai	System-level security, compliance, and infrastructure
App	meetings, templates, pdf	Business-specific features

Only two modules use `@Global()` (PrismaModule, LoggerModule); all other dependencies must be explicitly imported.

EVIDENCE The architecture documentation shows a clear separation between 18 core modules (security, compliance, infrastructure) and 3 app modules (business logic), with explicit dependency management preventing hidden cross-module access. Show Me

Admin Portal Separation

The admin portal operates as an independent application on separate ports (server: 4000, client: 4100), providing structural separation between administrative and operational functions.

EVIDENCE The admin portal is deployed as an independent full-stack application with its own server and client, providing structural separation of administrative duties from the main application. Show Me

Organizational & Process Controls

1. Policies & Documents

DOCUMENT	PURPOSE	OWNER	REVIEW CADENCE
[Organizational Chart — maintained by [HR],	Visual representation of reporting lines, department structure, and	[CHRO / CEO]	Semi-annual

DOCUMENT	PURPOSE	OWNER	REVIEW CADENCE
reviewed Semi-annually]	key positions with security responsibilities highlighted		
[Job Descriptions with Security Responsibilities — maintained by [HR / Security], reviewed Annually]	Each role includes specific security responsibilities aligned with the employee's system access level and organizational authority	[HR Director / CISO]	Annual
[Delegation of Authority Matrix — maintained by [Legal / Finance], reviewed Annually]	Specifies approval authorities for financial transactions, system changes, access provisioning, and policy exceptions by role and dollar/risk threshold	[CFO / General Counsel]	Annual
[RACI Matrix for Key Controls — maintained by [GRC Team], reviewed Annually]	Maps Responsible, Accountable, Consulted, and Informed roles for each key internal control activity	[CISO / GRC Manager]	Annual

2. Control Activities

ACTIVITY	FREQUENCY	RESPONSIBLE PARTY	OUTPUT/DELIVERABLE
Organizational chart update	Semi-annual / Per-event	[HR]	Updated organizational chart
Job description review and update	Annual	[HR / Hiring Managers]	Updated job descriptions
Delegation of authority review	Annual	[Legal / Finance / CISO]	Updated delegation matrix
RACI matrix update for control changes	Per-event / Annual	[GRC Team]	Updated RACI matrix
New role security responsibility briefing	Per-event (promotion/transfer)	[HR / Security Team]	Acknowledgement of new security responsibilities
Reporting line change impact assessment	Per-event	[HR / CISO]	Impact assessment for access and authority changes

3. Monitoring & Enforcement

- **Monitoring method:** [HR] maintains current organizational charts and notifies [CISO / GRC Team] of structural changes. RBAC role assignments are audited quarterly against organizational chart to confirm alignment. The system enforces role authorities at every request via the guard pipeline
- **Escalation procedures:** Structural changes affecting security-relevant positions are communicated to [CISO] within [5 business days] for access review. Misalignment between RBAC roles and organizational authority is escalated to [HR / CISO] for remediation
- **Consequence of non-compliance:** Access that does not align with documented organizational authority is revoked pending review. Departments that fail to maintain current job descriptions with security responsibilities are flagged for remediation

4. Key Artifacts for Auditors

- [ ] Current organizational chart with security-relevant positions highlighted
- [ ] Sample job descriptions showing security responsibility assignments (for key roles)
- [ ] Delegation of Authority Matrix (current version)
- [ ] RACI Matrix for key internal controls
- [ ] Evidence of organizational chart updates during the audit period
- [ ] RBAC role assignment report mapped to organizational positions

---

CC1.4 — Commitment to Competence

COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Control Objectives

The organization hires qualified personnel, provides ongoing security training, maintains competency standards for security-relevant roles, and evaluates performance against those standards.

Implemented Controls

Mandatory MFA for Privileged Roles

The system enforces mandatory MFA with role-specific policies, ensuring privileged users maintain heightened security competencies:

ROLE	MFA GRACE PERIOD	ENFORCEMENT
SuperAdmin	`always` (0-day — immediate)	Cannot access system without MFA

ROLE	MFA GRACE PERIOD	ENFORCEMENT
Admin	`always` (0-day — immediate)	Cannot access system without MFA
Consultant	`7_days`	Must set up MFA within 7 days
Leadership	`14_days`	Must set up MFA within 14 days
Customer	`never`	MFA optional
Unapproved	`never`	MFA optional

MFA adoption is monitored via admin metrics endpoint showing adoption rate, method distribution, and enrollment counts.

> **EVIDENCE** The MFA system enforces mandatory MFA with role-differentiated grace periods — SuperAdmin and Admin roles require immediate MFA setup, demonstrating that privileged access requires demonstrated competence with security controls. Show Me

Strong Password Policy Enforcement

The system enforces password complexity requirements that ensure credential competency:

REQUIREMENT	VALUE
Minimum Length	12 characters (registration), 8 characters (change)
Maximum Length	128 characters
Uppercase	At least 1 (A-Z)
Lowercase	At least 1 (a-z)
Special Characters	At least 1
History	5 previous passwords checked

> **EVIDENCE** The authentication system enforces comprehensive password policies including minimum length, complexity requirements, and password history — ensuring all users maintain credential hygiene standards. Show Me

First-User Bootstrap with Role Escalation

The system implements a structured onboarding path for the initial administrative user:

1. First registered user is automatically promoted to SuperAdmin
2. All subsequent users are assigned Unapproved role (zero-trust default)
3. Admin must explicitly approve and assign appropriate roles
4. Role changes are logged as audit events (`USER_ASSIGNED_TO_ORG` , `USER_ROLE_CHANGED`)

> **EVIDENCE** The RBAC system implements a zero-trust onboarding model where new users default to Unapproved status, requiring explicit Admin approval and role assignment — ensuring personnel are vetted before receiving access. Show Me

Organizational & Process Controls

1. Policies & Documents

DOCUMENT	PURPOSE	OWNER	REVIEW CADENCE
[Hiring Standards and Screening Policy — maintained by [HR], reviewed Annually]	Defines minimum qualifications, background screening requirements, and competency standards for security-relevant positions	[HR Director]	Annual
[Security Awareness Training Program — maintained by [Security / HR], reviewed Annually]	Establishes the training curriculum, delivery methods, frequency, and completion requirements for security awareness training	[CISO / HR Director]	Annual
[Certification and Continuing Education Policy — maintained by [HR / Security], reviewed Annually]	Specifies required certifications for security-relevant roles and continuing education requirements	[CISO / HR Director]	Annual
[New Hire Onboarding Checklist — maintained by [HR / IT], reviewed Annually]	Documents the complete onboarding process including security training, policy acknowledgement, access provisioning, and MFA setup	[HR Director / IT Manager]	Annual
[Performance Evaluation Criteria — maintained by [HR], reviewed Annually]	Includes security responsibility performance metrics for relevant roles	[HR Director / CISO]	Annual

2. Control Activities

ACTIVITY	FREQUENCY	RESPONSIBLE PARTY	OUTPUT/DELIVERABLE
Pre-employment background screening	Per-event (pre-hire)	[HR / Third-party screening vendor]	Completed screening reports
Security awareness training (all personnel)	Annual	[Security Team / HR]	Training completion records
Role-specific security training (privileged roles)	Annual	[Security Team]	Training completion records with competency verification
New hire onboarding with security orientation	Per-event	[HR / IT / Security]	Completed onboarding checklist
Performance evaluation with security metrics	Annual	[Managers / HR]	Performance review records
Security certification tracking	Ongoing	[HR / Security Team]	Certification inventory and expiration tracking
MFA setup verification for new privileged users	Per-event	[Security Team / System]	MFA adoption metrics and audit logs

3. Monitoring & Enforcement

- **Monitoring method:** [HR] tracks training completion rates with target of 100% within [30 days] of assignment. MFA adoption metrics are reviewed quarterly. The system automatically enforces MFA grace periods — privileged users who fail to set up MFA within their grace period are blocked from login
- **Escalation procedures:** Personnel who fail to complete required training within the deadline are reported to [Manager / HR Director]. Employees in security-relevant roles who lack required certifications are placed on remediation plans. Privileged users who fail to enable MFA within the grace period are automatically blocked by the system
- **Consequence of non-compliance:** System access is suspended for personnel who fail to complete mandatory security training or MFA setup. Continued non-compliance with certification requirements may result in role reassignment

4. Key Artifacts for Auditors

- ☐ Security awareness training materials (current curriculum)

- [ ] Training completion records for all personnel during the audit period
- [ ] Background screening completion records for new hires during the audit period
- [ ] New hire onboarding checklists (sample of completed checklists)
- [ ] Performance evaluation records showing security metrics (sample, anonymized)
- [ ] MFA adoption metrics showing privileged role compliance rates
- [ ] Certification inventory for security-relevant roles

CC1.5 — Accountability

COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Control Objectives

The organization assigns control ownership, measures performance against control responsibilities, tracks remediation of identified issues, and enforces accountability through escalation and consequence mechanisms.

Implemented Controls

User-Attributed Audit Logging

Every audit event includes attribution fields enabling individual accountability:

FIELD	PURPOSE
`userId`	Actor who triggered the event
`ipAddress`	Source IP (encrypted)
`userAgent`	Client identifier (encrypted)
`organizationId`	Organization context
`targetEmail`	Affected party (encrypted, deterministic for search)
`metadata`	Event-specific details (e.g., `originalRole`, `newRole`, `reason`)

EVIDENCE Every audit log entry includes userId, ipAddress, userAgent, organizationId, and event-specific metadata — enabling definitive attribution of every security-relevant action to a specific individual, IP, and device. Show Me

Alert Acknowledgement Tracking

The alerting system tracks accountability for deficiency response:

FIELD	PURPOSE
`sentAt`	When the alert notification was delivered
`acknowledgedAt`	When the responsible party acknowledged the alert
`acknowledgedBy`	User ID of the admin who acknowledged

Alert lifecycle: `PENDING → SENT → ACKNOWLEDGED`

> **EVIDENCE** The alerting system records who acknowledged each alert and when, providing auditable evidence of accountability for responding to control deficiencies. Show Me

Mandatory Reason for Administrative Overrides

When administrators perform sensitive actions (e.g., disabling user MFA), the system requires a documented reason:

- `MFA_ADMIN_OVERRIDE` audit event captures: admin user ID, target user ID, and mandatory reason text
- This override triggers a CRITICAL-severity alert
- The reason becomes part of the immutable audit record

> **EVIDENCE** The MFA system requires a mandatory reason when an admin disables a user's MFA, logged as an MFA_ADMIN_OVERRIDE event with CRITICAL alert severity — enforcing documented justification for security control overrides. Show Me

Role-Based Control Enforcement

The guard pipeline enforces accountability by ensuring every request is validated against the actor's assigned role:

```
Request → ThrottlerGuard (rate limit) → JwtAuthGuard (identity) → RbacGuard (authorization)
```

Every access attempt is validated in sequence — there is no bypass path for authenticated users.

EVIDENCE The architecture implements a mandatory guard pipeline (ThrottlerGuard → JwtAuthGuard → RbacGuard) that validates identity and authorization on every request, ensuring individuals can only perform actions within their assigned authority. Show Me

Organizational & Process Controls

1. Policies & Documents

DOCUMENT	PURPOSE	OWNER	REVIEW CADENCE
[Control Owner Assignment Matrix — maintained by [GRC Team], reviewed Annually]	Maps each internal control to a designated control owner responsible for its design, operation, and remediation of deficiencies	[CISO / GRC Manager]	Annual
[Performance Metrics Policy — maintained by [HR / GRC], reviewed Annually]	Defines how control responsibilities are incorporated into performance evaluations, including specific metrics for security-relevant roles	[HR Director / CISO]	Annual
[Escalation Procedures Document — maintained by [GRC Team], reviewed Semi-annually]	Documents the escalation path for unresolved control issues, remediation delays, and accountability failures	[CISO / GRC Manager]	Semi-annual
[Remediation Tracking Policy — maintained by [GRC Team], reviewed Annually]	Establishes the process for tracking remediation of identified control deficiencies from identification through verified closure	[GRC Manager / CISO]	Annual

2. Control Activities

ACTIVITY	FREQUENCY	RESPONSIBLE PARTY	OUTPUT/DELIVERABLE
Control owner assignment review	Annual	[GRC Team / CISO]	Updated Control Owner Assignment Matrix
Control owner self-assessment	Annual	[Control Owners]	Completed self-assessment questionnaires
Performance review with security metrics	Annual	[Managers / HR]	Performance evaluations incorporating control responsibilities

ACTIVITY	FREQUENCY	RESPONSIBLE PARTY	OUTPUT/DELIVERABLE
Remediation status review	[Weekly / Bi-weekly]	[GRC Team / Remediation Owners]	Updated remediation tracker
Escalation review for overdue items	Weekly	[GRC Manager]	Escalation notices for overdue remediations
Alert response time audit	Monthly	[Security Operations / GRC]	Report on alert acknowledgement timeliness

3. Monitoring & Enforcement

- **Monitoring method:** The automated alert acknowledgement system tracks response times for each alert by severity. [GRC Team] reviews remediation tracker weekly for overdue items. Control owner self-assessment completion is tracked annually. Performance evaluations incorporate security responsibility metrics
- **Escalation procedures:** Remediations overdue by [30 days] are escalated from [control owner] to [CISO]. Remediations overdue by [60 days] are escalated to [Executive Leadership]. CRITICAL alert acknowledgements exceeding [4-hour] SLA are escalated to [CISO]. Persistent accountability failures are reported to [Board / Audit Committee]
- **Consequence of non-compliance:** Control owners who fail to remediate assigned deficiencies within agreed timelines receive formal notification and increased monitoring. Repeated accountability failures are reflected in performance evaluations. Sustained non-compliance may result in reassignment of control ownership and reporting to [Executive Leadership]

4. Key Artifacts for Auditors

- ☐ Control Owner Assignment Matrix (current version)
- ☐ Control owner self-assessment results for the audit period
- ☐ Performance evaluation records showing security responsibility metrics (sample, anonymized)
- ☐ Remediation tracker showing deficiency assignment, progress, and closure
- ☐ Alert acknowledgement records showing response times for CRITICAL and HIGH alerts
- ☐ Escalation records for overdue remediations during the audit period
- ☐ Evidence of administrative override justifications (MFA_ADMIN_OVERRIDE audit logs)

Compliance Mapping

CRITERIA	COSO PRINCIPLE	TECHNICAL CONTROLS	ORGANIZATIONAL CONTROLS	STATUS
CC1.1	Principle 1 — Integrity and ethical values	26 audit event types with immutable storage, user enumeration prevention, self-serving action prevention, 46-pattern sensitive data sanitization	Code of Conduct, ethics hotline, background checks, disciplinary policy, annual acknowledgement	Technical: Implemented
CC1.2	Principle 2 — Board oversight	RBAC-scoped oversight access (SuperAdmin visibility), automated CRITICAL/HIGH alerting	Board charter, meeting cadence, independence assessment, control effectiveness reporting	Technical: Implemented
CC1.3	Principle 3 — Structure and authorities	6-level role hierarchy, multi-tenant organization scoping, core/app module separation, admin portal separation	Org chart, job descriptions, delegation of authority matrix, RACI matrix	Technical: Implemented
CC1.4	Principle 4 — Commitment to competence	Mandatory MFA with role-specific enforcement, password policy enforcement, zero-trust onboarding (Unapproved default)	Hiring standards, security training, certification policy, onboarding checklist, performance evaluations	Technical: Implemented
CC1.5	Principle 5 — Accountability	User-attributed audit logging, alert acknowledgement tracking, mandatory override justification, guard pipeline enforcement	Control owner matrix, performance metrics, escalation procedures, remediation tracking	Technical: Implemented

Gap Summary

GAP ID	CRITERIA	SEVERITY	DESCRIPTION
CC1-G1	CC1.1	High	No Code of Conduct document or annual acknowledgement process
CC1-G2	CC1.1	High	No ethics hotline or anonymous reporting mechanism
CC1-G3	CC1.2	High	No board or oversight committee charter documenting independence requirements and meeting cadence
CC1-G4	CC1.2	High	No evidence of board-level review of internal control effectiveness
CC1-G5	CC1.4	High	No formal security awareness training program or completion tracking
CC1-G6	CC1.1	Medium	No formal background check policy or pre-employment screening process
CC1-G7	CC1.3	Medium	No organizational chart with security responsibilities documented
CC1-G8	CC1.3	Medium	No delegation of authority matrix or RACI for key controls
CC1-G9	CC1.4	Medium	No formal hiring standards document for security-relevant positions
CC1-G10	CC1.4	Medium	No onboarding checklist integrating security orientation with system access provisioning
CC1-G11	CC1.5	Medium	No control owner assignment matrix mapping controls to responsible individuals
CC1-G12	CC1.5	Medium	No performance evaluation criteria incorporating security control responsibilities

---

Referenced Documentation

DOCUMENT	SCOPE	LINK
Infrastructure	SSH hardening, network security, disk encryption	Show Me

DOCUMENT	SCOPE	LINK
Architecture	Module separation, guard pipeline, admin portal separation	Show Me
Authentication	Password policies, account lockout, user enumeration prevention, rate limiting	Show Me
MFA	Mandatory MFA policies, role-specific grace periods, admin overrides, adoption metrics	Show Me
RBAC	Role hierarchy, organization scoping, SuperAdmin protections, self-serving action prevention	Show Me
Encryption	Data classification, sensitive data handling	Show Me
Logging	Audit events, alert pipeline, acknowledgement tracking, sensitive data sanitization, retention	Show Me