

TECHNOLOGY SERVICES

SOX Compliance Playbook

For eCommerce Retailers

How a leading US electronics retailer got SOX-ready — and what your team can learn from it.



What Is SOX - and Why Does It Matter for eCommerce?

The Short Version

The Sarbanes-Oxley Act (SOX) was born out of corporate scandals like Enron. It requires publicly listed companies to prove their financial reporting is accurate — and that the IT systems feeding those reports are under tight control.

For an electronics retailer, that means every online transaction, every inventory update, every pricing change — all of it has to be traceable, auditable, and change-controlled.

The key section? Section 404.



Section 302

CEO/CFO personally certify financial controls



Section 404

Annual audit of internal controls over financial reporting



IT General Controls

The IT layer that auditors examine most closely

The Four Pillars of IT General Controls

Everything SOX auditors will look at in your eCommerce platform

01



Change Management

Every code deploy, config change, and hotfix must be requested, approved, tested, and logged.

02



Logical Access

The right people get the right access. Developers don't touch production. Period.

03



Computer Operations

Monitoring, backups, incident response — your platform stays up and recoverable.

04



Financial Reporting Risk

The IT controls that protect the numbers flowing into your P&L and balance sheet.

Pillar 1: Change Management

Every change — from a homepage redesign to a backend patch — follows the same governed process



Real example from our electronics retailer:



When the team needed to migrate from Client-Side Rendering (CSR) to Server-Side Rendering (SSR) for SEO — a major architectural change — they didn't just deploy it. The change request went through evaluation (risk: high), authorization by the CAB, a full test plan covering regression, performance, and accessibility, and only then hit production. The audit trail lives in Jira, Git, and Jenkins automatically.

What Auditors Actually Check in Change Management



Every change approved before work starts

No developer begins coding until a Jira ticket is raised, risk-assessed, and authorized. The CAB (Change Advisory Board) signs off before anything goes to production.



Segregation of duties is enforced in code

Developers cannot merge their own pull requests. A peer reviewer — or independent QA — must approve every change before it merges to the main branch in Git/BitBucket.



Automated merge notifications

When any code merges to the codebase, the team gets an automated alert. This prevents silent, undetected changes — a key auditor concern.



Rollback plans are mandatory

For changes that can't be fully tested pre-production (e.g. data migrations), a documented rollback procedure is required before deployment approval.



Code scanning before every release

Automated vulnerability scanning runs on every release candidate. If a critical issue is found, the release is blocked. Logging framework and Spring framework vulnerabilities were caught and patched this way.

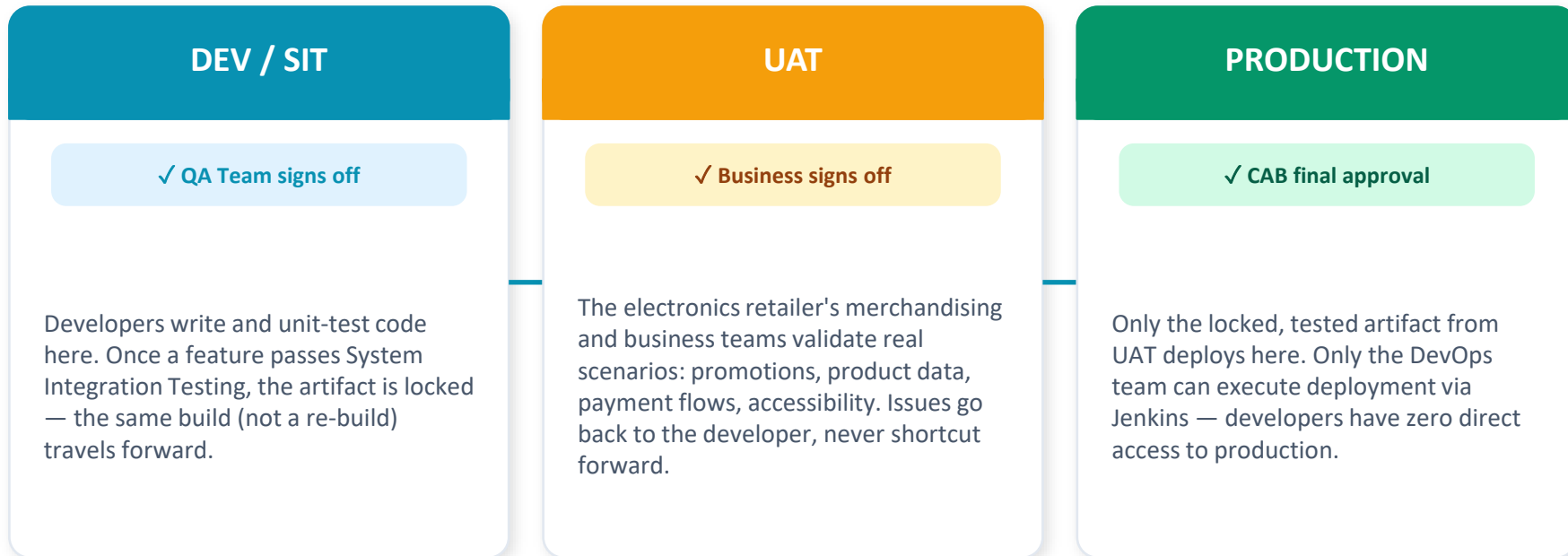


Emergency changes don't escape the process

Even a 2am hotfix gets documented and approved — after the fact but within a defined timeframe. No change is invisible.

Environment Separation: The Auditor's First Test

No code goes straight to production. Every release travels through three controlled gates.



Auditor note: These environments are maintained to be as identical as possible in hardware, software versions, and patches — so test results in UAT are a true proxy for production behaviour.

Pillar 2: Logical Access — Who Can Touch What?

For SOX, access control isn't just good security — it's a control that gets tested every audit cycle.

Role-Based Access Control (RBAC)



Every system role is defined with specific permissions on specific workspaces and APIs. A developer role cannot execute production deployments. A content editor cannot touch the codebase. Roles are reviewed and re-certified periodically.

VPN-only production access



The Gateway Microservice — the single entry point for all eCommerce microservices — is internally load-balanced. No external party can reach it without VPN whitelist approval. This is a hard technical control, not just a policy.

Offboarding is automatic



JumpCloud tracks every employee device and account. When someone leaves, their accounts are terminated from the directory within a defined window. Auditors want to see no orphan accounts with active access.

Multi-Factor Authentication everywhere



MFA is enforced organisation-wide. Password complexity rules are set centrally through JumpCloud. Auditors will pull evidence of MFA enforcement — it needs to be a configuration, not a recommendation.

Security Controls That Auditors Expect to See

OWASP Top Risks — How the Platform Is Protected

XSS Attacks

Input validation + Angular/React sanitization + HTTPS

SQL Injection

Persistent entities avoid direct SQL; parameterised queries

Broken Access Control

JWT tokens + single gateway entry point + RBAC

Sensitive Data Exposure

SSL everywhere; PCI data in Compass gateway only

Security Misconfiguration

K8s secrets + ConfigMaps; no hardcoded credentials

Known Vulnerabilities

GitHub scanning on every build; blocking release if critical



3 Isolated GCP Environments

Dev, QA, and Production are separate GCP projects with granular IAM permissions. CloudOps engineers are the only humans with production project access.



Akamai WAF + DDoS Protection

All public traffic goes through Akamai. The WAF blocks malicious requests before they reach the origin. Akamai Bot Manager handles scrapers & credential-stuffing bots - a real threat for retail.



Bi-weekly Security Patching

Kubernetes nodes are patched to the latest release in every two-week sprint cycle. GCP's auto-patching is disabled — patches are applied in a controlled, auditable manner.

Pillar 3: Computer Operations & Platform Health

Auditors want to see that you know when something breaks — and that you can recover.

Monitoring Stack

Telemetry

Real-time response time, Apdex score, throughput, and error rate across microservices

Kafka + Prometheus + Grafana

Kafka broker health — producers, consumers, and cluster metrics visualised in Grafana dashboards

Google Cloud SQL Insights

Storage usage, CPU/memory, read/write ops and ingress/egress tracked per instance

Penetration Testing

Regular external pen tests (Beadwindow) to identify exploitable vulnerabilities before attackers do



Data Backup & Recovery

- Automated daily backups within a 4-hour window
- 3-day retention policy with backups stored separately from the Cloud SQL instance
- Restore procedures tested — not just documented



Remote Work Controls

- VPN for all remote connections
- Endpoint protection: antivirus, auto-patching, full disk encryption
- Asset inventory via JumpCloud: every device, OS version, and user tracked

The Audit Trail: Traceability from Code to Cash

SOX auditors will trace a change all the way from the business requirement to production. Here's how that works in practice.



Requirement
(Jira Story)



Code Commit
(Git / BitBucket)



Test Results
(Selenium / Katalon)



Deployment
(Jenkins CI/CD)



Change Request
(ITSM Ticket)

What full traceability looks like for the electronics retailer:

- When a developer commits code in Git, the linked Jira story automatically updates with the changeset and commit message.
- When Jenkins deploys to production, a new change request is automatically created in the ITSM tool — zero manual logging.
- When a Selenium test fails, a defect is auto-created in Jira. When a code scan fails, same. Every failure is traceable.
- When a performance monitoring tool detects slowdown, a defect is created in the ALM tool with context — before a customer calls.

Data Security, PCI & Privacy

For an electronics retailer, protecting customer payment data and privacy isn't optional — it's audited.



Encryption at Rest

All databases (PostgreSQL, Cassandra) and backups are encrypted. Datafiles, temp files, and backup files — all encrypted. This is verified during the audit by examining GCP configurations.



Encryption in Transit

All data in motion uses SSL — from the browser to Akamai, and internally within GCP. No plaintext communication permitted anywhere in the stack.



PCI Data Isolation

Card data never touches the core platform. Payment processing goes through a PCI-compliant gateway (Compass). The eCommerce platform doesn't store, transmit, or process raw card data — this dramatically reduces PCI scope.



PII & Log Hygiene

Application logs are designed to never capture PII or PCI data. This is a code-level control, not just policy — log output is reviewed during code review.



GDPR & CCPA Compliance

The platform exposes CRUD operations for customer data and fires events to other systems on data changes — so right-to-erasure and data portability requests can be fulfilled. Consent is captured and stored correctly.



Secrets & Key Management

Application credentials are stored as Kubernetes secrets, never in code or config files. Passwords in the database use one-way SHA1 encryption. Auditors examine this to ensure no hardcoded credentials exist anywhere.

Governance: Who Owns What in a SOX Audit

SOX isn't just about having controls — it's about being able to show who is responsible for each one.

R Responsible
Does the work

A Accountable
Owns the outcome

C Consulted
Provides input

I Informed
Kept in the loop

Activity	Customer	Project Director	Solution Architect	Change Manager	DevOps
Identify scope change	I	A	C	R	I
Submit change request	R	I	I	A	I
Assess change request	C	C	R	C	C
CAB Board Review	C	A	C	R	C
Change Approval/Disposition	A	C	C	C	I
Deploy to production	I	I	C	A	R

Agile + SOX: They're Not Enemies

A common myth: moving fast breaks compliance. Our electronics retailer went from quarterly releases to daily production deploys — while staying fully SOX-compliant.



How do you move this fast and stay compliant?



CI/CD Automation

Jenkins automates build, test, and deploy. Every step is logged automatically — no manual audit trail to maintain.



Test Automation

Selenium, Katalon, Cucumber — regression suites run on every commit. Auditors see test evidence, not just assertions.



Config Management

Infrastructure as code. Kubernetes ConfigMaps and secrets mean no ad-hoc configuration changes — every change is in source control.



Granular Backlog

A well-structured Jira backlog means every sprint item maps to a business requirement. Traceability is built into the workflow.

Your SOX Audit Readiness Checklist

Before your auditors arrive, make sure you can say yes to all of these.

Change Management

- Every change has a Jira ticket with risk, priority, and approval documented
- No developer can merge their own pull request (enforced in Git)
- Separate DEV, UAT, and PROD environments with defined sign-off owners
- Post-implementation reviews are logged for production changes

Security & Ops

- Vulnerability scanning runs on every release candidate
- WAF and DDoS protection is in place (Akamai or equivalent)
- Automated daily backups with tested restore procedures
- Pen testing has been conducted in the last 12 months

Logical Access

- RBAC is configured — no developer has direct production write access
- MFA is enforced (not just recommended) for all systems
- Joiners/leavers process terminates access within a defined SLA
- Access is reviewed and re-certified at least annually

Data & Privacy

- PCI card data never stored in your platform — gateway handles it
- Encryption at rest and in transit verified in GCP config
- PII is not captured in application logs
- GDPR/CCPA data deletion workflow is implemented and tested

Pillar 4: Financial Reporting Risk

This pillar is the retailer's responsibility — but AIE's work makes it possible.

What Pillar 4 Covers



GL Reconciliation

Revenue from the eCommerce platform must reconcile to the general ledger. Every order, refund, and discount needs to land correctly in your ERP (SAP, Oracle, NetSuite).



Revenue Recognition

Under ASC 606, revenue is recognised when control of goods transfers. Your finance team defines the rules; the platform must implement them correctly.



Management Review Controls

Finance leadership must review and sign off on financial reports — analytical reviews, variance analysis, and period-end close procedures.



CFO/CEO Certification

Under SOX Section 302, your CEO and CFO personally certify financial statement accuracy. Everything below — including the eCommerce platform — feeds that certification.

Your Responsibility



- Finance & Internal Audit team
- ERP configuration & GL mapping
- Period-end close & management review
- CFO/CEO SOX certifications

How AIE Enables It



- Auditable transaction logs for every order
- Change-controlled pricing & promotions logic
- Reliable, traceable data pipelines to your ERP
- Secure platform that auditors can rely on

Think of it this way: AIE makes the data trustworthy. Your finance team certifies it. Both sides must hold.

Ready to Get SOX-Ready?

AIE has helped a leading US electronics retailer achieve full SOX compliance while accelerating from quarterly to daily production releases. We can do the same for you.



SOX Readiness Assessment

We audit your current controls against ITGC requirements and give you a gap report.



Control Implementation

We build the processes, tooling, and governance structures that satisfy auditors.



Agile + Compliance Design

We design your SDLC so compliance is built in — not bolted on after the fact.



Ongoing Audit Support

We provide evidence packs, walkthroughs, and remediation support each audit cycle.

 sales@aienterprise.com |  www.aienterprise.com |  +1 833-234-0247