Network Infrastructure and Security Plan for Nozama

Posted on October 9, 2018

Nozama is a fictional online retailer that sells printed books and e-books and therefore depends on a secure, resilient, and scalable network infrastructure. The original plan correctly identified web, email, file, and database services; the need to choose server locations; hardware and software requirements; implementation cost; and protection of customer information. A modern design should avoid building every function on separately purchased physical servers without considering cloud platforms, managed services, identity controls, backup, payment-card scope, and continuous monitoring. The recommended architecture is hybrid and vendor-neutral: customer-facing services run in a well-governed cloud environment across multiple availability zones, while office devices and any local operational systems connect through secured networks and identity-based access. Nozama should minimize the cardholder data it stores, use a compliant payment provider, encrypt sensitive information, segment systems, and design recovery before launch. (National Institute of Standards and Technology, 2024)

Business and Technical Requirements

The infrastructure must support product browsing, search, customer accounts, shopping carts, payments, order management, e-book delivery, customer service, inventory information, analytics, marketing communication, and employee collaboration. Nonfunctional requirements include availability, performance, confidentiality, integrity, scalability, accessibility, maintainability, and regulatory compliance. Demand may rise sharply during promotions or holidays, so the architecture should scale automatically instead of relying on permanently oversized hardware. Because book sales and digital downloads occur continuously, the company should define service-level objectives such as acceptable page-load time, monthly availability, maximum recovery time, and maximum data loss after disruption.

Architecture Overview

The proposed system separates the public application, internal administration, data layer, and office environment. Internet users reach Nozama through a domain-name service, content-delivery network, distributed denial-of-service protection, and web application firewall. Requests then pass to a load balancer serving application instances or containers in at least two availability zones. Databases and object storage remain in private network segments inaccessible directly from the internet. Administrative access requires strong identity verification through a controlled management path.

The office network is segmented from production and connects through encrypted, authenticated channels. Logs from cloud, endpoints, identity systems, applications, and payment workflows are collected centrally for detection and investigation.

Cloud, On-Premises, or Hybrid Deployment

The original plan considered whether servers should be placed at the company site or hosted elsewhere. For a new online retailer, a cloud-first production environment is generally preferable because it provides geographic redundancy, elastic capacity, managed databases, object storage, monitoring, and security services without the capital cost of a private data center. This does not transfer all responsibility to the provider. Nozama remains responsible for configuration, identity, applications, data, and compliance under the shared-responsibility model. A small local environment may still support office printing, network services, point-of-sale functions if a physical shop exists, or cached operational tools. The result is hybrid because business users and devices operate locally while production services run in the cloud.

Public Web Application

The web application should use a supported framework, secure coding standards, automated testing, and a deployment pipeline that separates development, testing, and production. Static assets such as images, style files, and downloadable public documents can be delivered through a content-delivery network. Dynamic requests are processed by stateless application instances that can be added or removed according to demand. Session data should not depend on one server. A web application firewall can block common malicious patterns, but it cannot correct vulnerable code. Input validation, output encoding, secure headers, dependency management, authentication, authorization, and business-logic testing remain essential.

Mobile and API Access

If Nozama later offers mobile applications or external partner integrations, they should use versioned APIs protected by an API gateway. Each client receives only the functions and data it requires. Tokens should be short-lived and validated, rate limits should reduce abuse, and sensitive actions may require stronger verification. API documentation must not expose secrets. Inventory, pricing, order, and customer endpoints should apply authorization at the object level so one customer cannot access another customer’s records by changing an identifier. Automated security testing should include APIs because attackers may bypass the visible website.

Identity and Access Management

Identity is the foundation of the architecture. Customers need secure account registration, sign-in, recovery, and optional multifactor authentication. Employees and administrators should use a centralized identity provider with phishing-resistant multifactor authentication for privileged roles. Role-based access limits employees to the functions necessary for their duties, while just-in-time privilege can reduce permanent administrative access. Shared accounts should be prohibited. Joiner, mover, and leaver processes must create, update, and disable access promptly as employment changes. The zero-trust principle is that access is evaluated according to identity, device, context, and resource rather than trusted merely because a user is inside the office network. (National Institute of Standards and Technology, 2020, 2025)

Customer Authentication

Customer passwords must be protected with a modern adaptive password-hashing algorithm and never stored in readable form. The site should support long passwords and password managers rather than impose confusing composition rules. Rate limiting, bot detection, breached-password screening, and risk-based challenges help reduce credential stuffing. Account recovery is a common weakness and should use verified channels, short-lived tokens, notification of changes, and protection against social engineering. Multifactor authentication should be encouraged, especially before changing payment, email, or delivery information. Authentication controls should remain usable and accessible so that security does not push customers toward unsafe workarounds.

Network Segmentation

Segmentation limits the movement of an attacker and reduces compliance scope. Public load balancers are placed in an internet-facing segment, application workloads in private segments, and databases in still more restricted segments. Security groups or firewall rules permit only required flows and deny all others by default. Development and testing environments are separated from production, and production data should not be copied into lower environments unless properly anonymized. The office network uses separate virtual LANs or equivalent controls for employee devices, voice systems, printers, guest Wi-Fi, Internet of Things devices, and any local servers. Guest devices receive internet access but no route to corporate resources.

Office Network

The office requires business-grade firewalls, managed switches, centrally administered wireless access points, redundant internet service where justified, and secure remote access. WPA3-Enterprise or a current enterprise wireless standard with individual authentication is preferable to a shared office

password. Network equipment should be inventoried, patched, backed up, and configured through controlled administration. Printers and other embedded devices often receive less attention and should be isolated. Employees working remotely access applications through identity-aware gateways, secure access service edge technology, or a well-managed virtual private network according to risk. Connecting from an unmanaged personal device should not automatically provide the same access as a compliant company endpoint.

Database Services

The transaction database stores customer profiles, catalog data, carts, orders, payment references, inventory, and fulfillment status. A managed relational database is suitable for transactional consistency and can provide automated backups, patching, encryption, replication, and failover. Read replicas or caching may improve performance, while search can be handled by a separate indexed service. Database credentials should be obtained from a secrets-management system and rotated, not placed in application code. Queries should use parameterization to prevent injection. Administrative access is limited, logged, and performed through approved tools. Data classification determines which fields require additional masking or tokenization.

E-Book Storage and Delivery

E-book files should be stored in encrypted object storage rather than served from a shared file server. The application can generate time-limited, customer-specific download links after verifying purchase rights. This approach reduces direct exposure of storage and supports scale. Digital-rights management may be considered according to publisher contracts, but it should be balanced against accessibility, customer ownership expectations, and interoperability. Download events should be logged, and unusual automated retrieval can trigger review. Backup and versioning protect against deletion or ransomware, but storage permissions remain the primary control.

Payment Security and PCI DSS

Nozama should minimize its payment-card environment by using a reputable payment service provider that hosts or tokenizes sensitive payment entry. The company should not store card verification codes, and ideally it should store only provider tokens and limited transaction references. PCI DSS applies to entities that store, process, transmit, or can affect the security of payment account data. Using a provider reduces but does not eliminate obligations: the website, scripts, administrative accounts, policies, vulnerability management, and incident response can still affect payment security. The exact compliance path should be confirmed with the acquiring bank and qualified professionals. (PCI Security Standards Council, 2024)

Third-Party Scripts and Supply-Chain Risk

E-commerce pages often include analytics, advertising, chat, review, and personalization scripts. A compromised script can steal payment or customer information. Nozama should maintain an inventory of browser-side scripts, approve changes, use content security policy and integrity controls where practical, and monitor page behavior. Software dependencies and container images should be scanned for known vulnerabilities and obtained from trusted sources. Vendor risk reviews should cover security, privacy, availability, subcontractors, breach notification, data return, and termination. A trusted logo is not a substitute for contractual and technical verification.

Email and Collaboration

The original plan proposed a dedicated mail server. A managed business email and collaboration platform is usually safer and easier for a small retailer because it provides filtering, retention, availability, and administrative controls. The company must configure domain-based protections such as SPF, DKIM, and DMARC to reduce spoofing. Multifactor authentication is mandatory for employees, and external forwarding should be controlled. Customer transactional messages—receipts, password resets, and download notices—should be sent through a separate authenticated service so marketing activity does not damage critical email deliverability. Sensitive information should not be sent in plain email when a secure portal is available.

File and Document Management

Internal files such as contracts, publisher agreements, finance records, policies, and product assets should use a managed document platform with versioning, role-based access, retention, and audit history. A traditional open network share encourages uncontrolled copying and broad access. Documents should be classified, and highly sensitive records should receive additional restrictions. Public links require expiration and approval. Local storage on laptops should be minimized and protected through full-disk encryption and endpoint management. The system must support legal holds and retention requirements where relevant.

Endpoint Security

Company laptops and mobile devices should be enrolled in centralized management. Controls include full-disk encryption, automatic patching, endpoint detection and response, supported operating systems, screen locking, browser management, removal of local administrator rights, and remote wipe. Application allowlisting may be appropriate for high-risk roles. Employees should use separate work profiles rather than sharing devices with household members. Lost devices must be reportable immediately. Endpoint compliance can become an input to access decisions so that a device missing

critical patches cannot reach sensitive administration functions.

Secure Software Development

Nozama's development lifecycle should include threat modeling, code review, dependency scanning, static and dynamic testing, secrets detection, infrastructure-as-code review, and controlled release approval. Developers should not use production credentials or customer data on personal machines. Changes are tracked in version control and deployed through automated pipelines with rollback capability. Security defects are prioritized according to exploitability and business impact. Independent penetration testing provides additional evidence but does not replace daily secure development. The company should maintain a vulnerability disclosure process so researchers can report issues responsibly.

Encryption and Key Management

Data in transit should use current Transport Layer Security, while databases, storage, backups, and endpoints use encryption at rest. Encryption keys are managed separately through a cloud key-management or hardware security service, with limited access, rotation, audit, and recovery procedures. Secrets such as API keys, database passwords, and signing keys belong in a secrets vault rather than configuration files or email. Encryption protects stolen media and intercepted traffic but does not prevent misuse by an authorized compromised account. Identity, segmentation, and monitoring are still required.

Logging and Security Monitoring

Central logging should collect authentication, privilege changes, application errors, firewall events, web application firewall alerts, database administration, cloud control-plane actions, endpoint detections, payment events, and critical business actions. A security information and event management platform or managed detection service can correlate suspicious behavior. Logs need synchronized time, integrity protection, access control, and a defined retention period. Alerting should prioritize credible risks such as impossible travel, creation of privileged users, large data exports, disabled security controls, and unusual payment-page changes. Monitoring without staff or a service responsible for response creates false confidence. (OWASP Foundation, 2021)

Availability and Load Management

Public services should operate across more than one availability zone so that the failure of a data center does not stop sales. Load balancers perform health checks and direct traffic only to functioning instances. Auto-scaling responds to traffic, while caching and the content-delivery network reduce

origin load. Capacity limits and cloud quotas should be tested before major promotions. Graceful degradation can keep browsing available even if a recommendation or review service fails. Business continuity should distinguish essential checkout and fulfillment functions from optional features.

Backups

Nozama needs automated, encrypted, versioned backups with copies isolated from ordinary administrator credentials. The 3-2-1 principle—multiple copies, different media or systems, and at least one logically or geographically separate copy—is a useful starting point. Database point-in-time recovery, object versioning, infrastructure definitions, and document backups protect different assets. A backup is not proven until restoration is tested. Tests should verify data integrity, required keys, application compatibility, and the time needed to resume service. Ransomware-resistant or immutable storage can reduce the chance that an attacker deletes backups.

Recovery Objectives

Recovery time objective (RTO) defines how long a service can remain unavailable, while recovery point objective (RPO) defines how much recent data loss is tolerable. Checkout may require a short RTO and near-zero RPO, while an internal archive may tolerate longer recovery. These objectives determine architecture and cost. A disaster-recovery runbook should identify decision authority, communication, failover, restoration order, validation, and return to normal operation. Exercises should include cloud-region failure, ransomware, database corruption, identity-provider outage, and payment-provider disruption.

Incident Response

The incident-response plan covers preparation, detection, analysis, containment, eradication, recovery, communication, and lessons learned. Contact information for executives, legal counsel, insurers, cloud providers, payment partners, law enforcement, and forensic specialists should be maintained offline. The team needs authority to disable accounts, block traffic, isolate devices, or take the store temporarily offline. Evidence must be preserved, and notification duties vary according to data, location, contracts, and law. Prewritten communication templates reduce confusion but must be adapted honestly. Concealing an incident to protect reputation usually increases legal and trust damage.

Privacy and Data Governance

Nozama should collect only customer information required for transactions, delivery, support, legal obligations, and clearly explained personalization. Privacy notices must describe collection, sharing,

cookies, retention, and rights applicable to users. Marketing consent should be separate from essential service communication. Data should have owners, classifications, retention schedules, deletion procedures, and controlled access. Analytics datasets can use pseudonymization or aggregation. The company should avoid storing sensitive inferred interests unnecessarily, especially because reading history can reveal political, religious, health, and personal information.

Hardware Requirements

Because production is cloud-based, local hardware focuses on employee productivity and network resilience rather than a rack of public servers. Requirements include business-grade firewalls, managed switches, secure wireless access points, uninterruptible power for network equipment, company-managed laptops, approved mobile devices, barcode or fulfillment equipment if physical inventory is handled, and secure storage for spare devices. Redundancy should match business impact. Two diverse internet connections may be justified for an office that processes fulfillment continuously, while a small remote team may rely more on cloud access from alternate locations.

Software Requirements

Core software categories include an e-commerce application, content-management and catalog tools, managed database, object storage, search service, payment integration, customer-service platform, identity provider, endpoint-management system, code repository and deployment pipeline, monitoring, backup, document collaboration, accounting, inventory, and security tools. Vendor selection should consider support, data portability, integration, security documentation, cost at scale, and termination. Open-source software may reduce licensing expense but still requires skilled maintenance. Proprietary software may simplify operation but increase dependency. The company should avoid designing the entire architecture around a product that cannot be replaced.

Cost Model

The original paper listed one-time hardware prices that are likely to become outdated. A more useful budget separates capital and recurring categories. Initial costs include design, application development, testing, migration, employee devices, network equipment, legal and compliance review, and implementation services. Recurring costs include cloud compute and storage, payment fees, bandwidth, email, support platforms, monitoring, security services, backups, licensing, staff, insurance, penetration testing, and training. Cloud cost should be modeled under ordinary and peak traffic. Reserved capacity or savings plans may reduce predictable expense, while budgets and alerts prevent accidental consumption.

Governance and Responsibilities

Technology succeeds only when responsibility is assigned. A senior leader owns risk, a technical leader owns architecture and operations, a security lead coordinates controls and incidents, developers own secure code, and business owners approve access to data. Small companies may outsource some roles, but accountability cannot be outsourced. Policies should cover acceptable use, access, data handling, development, vendors, backups, incidents, and change management. Security awareness includes phishing, payment fraud, social engineering, password managers, and reporting. Metrics should track availability, recovery tests, patching, vulnerabilities, account reviews, incidents, and customer-impacting failures.

Implementation Roadmap

Phase one defines requirements, data classification, threat model, RTO/RPO, and provider selection. Phase two builds separate development and production environments through infrastructure as code, configures identity and network segmentation, and integrates a hosted payment flow. Phase three implements monitoring, backup, endpoint management, secure email, and incident procedures. Phase four performs performance, accessibility, security, restoration, and failover testing before launch. Phase five monitors real use, corrects issues, and conducts regular reviews. Major features should be released gradually through controlled deployment rather than changing every customer at once.

Conclusion

Nozama needs an infrastructure that supports continuous book sales and e-book delivery without exposing customer or payment data unnecessarily. A cloud-first hybrid design provides scalability and resilience, while private network segments, centralized identity, multifactor authentication, secure endpoints, managed databases, object storage, and continuous monitoring reduce risk. Payment processing should be delegated to a compliant provider and designed to minimize PCI DSS scope. The office network remains segmented, and employees access production according to identity and device trust rather than physical location. Backups, RTO/RPO, disaster recovery, and incident response are designed before failure. Cost should be evaluated through recurring service and staffing categories rather than obsolete server-price lists. The resulting network is not secure because of one firewall or brand; it is secure because architecture, software, people, and governance reinforce one another.

References

National Institute of Standards and Technology. (2020). *Zero trust architecture* (NIST SP 800-207).

National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0*.

National Institute of Standards and Technology. (2025). *Implementing a zero trust architecture* (NIST SP 1800-35).

OWASP Foundation. (2021). *OWASP Top 10: The ten most critical web application security risks*.

PCI Security Standards Council. (2024). *Payment Card Industry Data Security Standard: Requirements and testing procedures* (Version 4.0.1).