Zero Trust + Compliance Framework

A practical framework for connecting security architecture with governance, risk, and compliance.

SecureHops

Security for Startups & Scale-Ups

Use this framework to connect Zero Trust principles to practical security activities, evidence, ownership, and compliance planning.

Zero Trust and Compliance Solve Different Problems

Zero Trust is a security architecture and operating approach. Compliance frameworks are governance and assurance mechanisms. They are related, but they are not interchangeable.

Zero Trust Asks:

- "How should access to resources be designed and enforced?"
- Protect resources regardless of network location
- Verify explicitly before granting access
- Assume breach and minimize blast radius

Compliance Asks:

- "How do we establish, govern, operate, and demonstrate that our security practices meet applicable requirements?"
- Define governance structures and policies
- Identify and manage risk
- Produce evidence that controls operate as intended

They Can Work Together

Zero Trust practices can strengthen the implementation of security controls that also support compliance objectives.

Example: Requiring MFA and least-privilege access (Zero Trust) can provide evidence for access-control design, authentication enforcement, access reviews, and privileged-access management (compliance).

Zero Trust can support compliance work — but it does not automatically satisfy any specific compliance framework. Each framework has its own scope, requirements, and evidence expectations.

The Six Zero Trust Areas

These are practical organizing categories inspired by Zero Trust architecture principles and related implementation guidance. They are not official NIST pillar terminology.

1. Identity

Ensure access decisions are tied to verified identities and appropriate authorization. Centralized identity, MFA, lifecycle management, and privileged-access controls.

2. Devices / Endpoints

Establish appropriate trust signals for devices accessing sensitive resources. Endpoint inventory, device management, security configuration, and patching.

3. Applications & Workloads

Protect applications, services, APIs, and workloads through identity-aware controls and secure development practices. Service identities, secrets management, and production access controls.

4. Networks & Connectivity

Limit access based on explicit authorization rather than network location alone. Segmentation, identity-aware access, and secure remote access.

5. Data

Protect data based on sensitivity, business value, and authorized access. Classification, encryption, access restrictions, retention, and secure disposal.

6. Visibility & Analytics

Detect unusual or unauthorized activity and support continuous security decisions. Logging, monitoring, alerting, and incident detection.

Cross-Cutting: Governance & Automation

Policies, risk management, asset ownership, control ownership, exception management, access reviews, security metrics, incident management, vendor risk, change management, and evidence management.

The Framework Matrix

Zero Trust Area	Security Objective	Example Practices	Evidence You Could Maintain	Compliance / GRC Connection	Owner
Identity	Ensure access decisions are tied to verified identities and appropriate authorization.	Centralized identity, MFA, lifecycle management, privileged access controls, role-based access, access reviews.	Identity configuration, MFA configuration, access review records, joiner/mover/leaver records.	Access control, risk management, security governance.	
Devices / Endpoints	Establish appropriate trust signals for devices accessing sensitive resources.	Endpoint inventory, device management, security configuration, patching, endpoint protection.	Asset inventory, endpoint management records, patch reports, security configuration records.	Asset management, security operations, risk management.	
Applications & Workloads	Protect applications, services, APIs, and workloads through identity-aware controls.	Application authentication, API authorization, service identities, secrets management, production access controls.	Application access configuration, deployment records, secrets-management configuration.	Change management, access control, secure development.	
Networks & Connectivity	Limit access based on explicit authorization rather than network location alone.	Segmentation, identity-aware access, secure remote access, network policy.	Network policies, access policies, configuration records, remote-access records.	Access control, security operations, risk management.	
Data	Protect data based on sensitivity, business value, and authorized access.	Data classification, encryption, access restrictions, retention, secure disposal.	Data classification records, access reviews, encryption configuration, retention procedures.	Data protection, privacy, risk management.	
Visibility & Analytics	Detect unusual or unauthorized activity and support continuous security decisions.	Logging, monitoring, alerting, security analytics, incident detection.	Logs, monitoring configurations, alerts, incident records, review records.	Monitoring, incident response, evidence management.	

Zero Trust Needs Governance

Technology alone does not create a sustainable Zero Trust program. Governance ensures that security decisions are documented, ownership is assigned, and evidence is maintained.

Governance Layer Components

- Policies — Document security requirements and expectations
- Risk management — Identify, assess, and treat security risks
- Asset ownership — Know who owns each system, service, and data set
- Control ownership — Assign responsibility for each security practice
- Exception management — Document and approve deviations from standards
- Access reviews — Periodically verify that access rights remain appropriate
- Security metrics — Track meaningful indicators of security-program health
- Incident management — Detect, respond to, and learn from security events
- Vendor risk — Assess and monitor third-party security
- Change management — Control and trace production changes
- Evidence management — Collect, organize, and retain proof that controls operate

The Relationship

Governance !’ Risk !’ Identity / Device / Application / Network / Data !’ Visibility !’ Review & Improvement

The goal is continuous decision-making rather than installing a collection of security products.

How Zero Trust Practices Can Support Compliance Work

This mapping shows where Zero Trust practices may connect to GRC activities. These are potential connections, not guarantees of framework compliance.

Zero Trust Practice	Potential GRC Connection	Possible Evidence	Framework Examples
MFA	Access control	Identity configuration, authentication policy	SOC 2 / ISO/IEC 27001
Least privilege	Access governance	Access review records, privilege records	SOC 2 / ISO/IEC 27001
Joiner / mover / leaver	User lifecycle management	Access tickets, HR workflow records	SOC 2 / ISO/IEC 27001
Privileged access management	Privileged access governance	Privileged account inventory, access reviews	SOC 2 / ISO/IEC 27001
Centralized logging	Monitoring / security operations	Log configuration, review records	SOC 2 / ISO/IEC 27001
Network segmentation	Risk reduction / system protection	Architecture diagrams, network policies	SOC 2 / ISO/IEC 27001
Secure application access	Application security / access control	Application config, authorization records	SOC 2 / ISO/IEC 27001
Data classification	Information governance	Classification records, data handling procedures	SOC 2 / ISO/IEC 27001
Incident detection	Incident response	Alerts, incident records	SOC 2 / ISO/IEC 27001
Vendor access controls	Third-party risk	Vendor reviews, access records	SOC 2 / ISO/IEC 27001

The 'Framework Examples' column indicates these practices may be relevant when addressing applicable requirements or criteria. This does not mean a practice automatically satisfies any specific framework.

A Practical Startup Implementation Model

Do not attempt to transform the entire environment at once. Start with critical resources and high-risk access paths.

Stage 1 — Know What You Have

- Users and identities
- Devices and endpoints
- Applications and workloads
- Data and its sensitivity
- Critical services and dependencies
- Privileged accounts
- Third-party dependencies

Stage 2 — Control Identity

- Centralized identity provider
- MFA for critical systems
- Lifecycle management (joiner/mover/leaver)
- Least-privilege access
- Privileged-access controls

Stage 3 — Protect Critical Resources

- Production systems
- Sensitive data stores
- Administrative interfaces
- Critical SaaS applications
- Cloud infrastructure

Stage 4 — Add Visibility

- Logging for important systems
- Monitoring and alerting
- Incident detection workflows
- Periodic security reviews

Stage 5 — Connect to Governance

- Document policies
- Record risk decisions
- Assign control ownership
- Collect and retain evidence
- Manage exceptions
- Conduct periodic reviews

Zero Trust + Compliance Self-Assessment

Use this checklist to review your current status. This is a self-assessment tool, not a scoring system.

Count how many areas you can answer 'Yes' or 'Partial' to. Use 'No' and 'N/A' to identify gaps requiring attention.

Area	Question	Yes	Partial	No	N/A	Owner	Next Action
Identity	Do all users have individual identities?						
Identity	Is MFA enforced for critical systems?						
Identity	Are privileged accounts identified?						
Identity	Are access rights reviewed periodically?						
Identity	Is access removed promptly when no longer required?						
Devices	Is there an inventory of managed devices?						
Devices	Are security configurations defined?						
Devices	Are important endpoints monitored?						
Devices	Are critical patches tracked?						
Applications	Are production applications identified?						
Applications	Are service accounts controlled?						
Applications	Are secrets managed securely?						
Applications	Is production access restricted?						
Networks	Are critical administrative interfaces protected?						
Networks	Is remote access controlled?						
Networks	Are sensitive resources separated where appropriate?						
Data	Is sensitive data identified?						
Data	Are data access permissions reviewed?						
Data	Is sensitive data protected appropriately?						
Data	Are retention and disposal practices defined?						
Visibility	Are important security events logged?						
Visibility	Are alerts monitored?						
Visibility	Are incidents tracked?						
Visibility	Are security events reviewed where appropriate?						
Governance	Does each important security practice have an owner?						
Governance	Are exceptions documented?						
Governance	Are risks tracked?						
Governance	Is evidence retained?						
Governance	Are security policies reviewed?						

Current Review Status — This is a self-assessment tool. Do not create a percentage score or readiness rating.

Build Security That Supports the Business

Zero Trust is most useful when it becomes part of how your organization manages access, protects critical resources, monitors risk, and demonstrates security — not when it becomes another collection of tools.

Get Your Security Assessment !' securehops.com/assessment
Book a 30-Min Security Call !' securehops.com/book

Sources & Further Reading

NIST SP 800-207 — Zero Trust Architecture
https://csrc.nist.gov/pubs/sp/800/207/final

NIST SP 1800-35 — Implementing a Zero Trust Architecture
https://www.nccoe.nist.gov/zero-trust-architecture

NIST SP 800-207A — Zero Trust Architecture Model for Access Control in Cloud-Native Applications
https://csrc.nist.gov/pubs/sp/800/207/a/final

CISA Zero Trust Maturity Model v2.0
https://www.cisa.gov/zero-trust-maturity-model

AICPA & CIMA — Trust Services Criteria
https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

ISO/IEC 27001:2022
https://www.iso.org/standard/27001

Do not imply these organizations endorse SecureHops. This framework references these sources for context and does not claim to be an official NIST, CISA, AICPA, or ISO framework.