QOS MSP Managed Services

HITRUST COMPLIANCE STRATEGY

A NO-NONSENSE GUIDE FOR IT LEADERS

+1 (877) 800-7672

www.qosmsp.com

HITRUST Compliance Strategy: A No-Nonsense Guide for Business Leaders

Many organizations approach HITRUST compliance as an audit project instead of an ongoing security and risk management program. The result is compliance gaps, audit challenges, increased risk exposure, and unnecessary operational complexity.

HITRUST is more than a certification. It is a comprehensive framework designed to help organizations manage security, privacy, compliance, and risk through a structured and measurable approach.

Use this framework to strengthen compliance readiness, improve security maturity, and build a sustainable compliance program.

1. Stop Treating HITRUST as a One-Time Certification

Achieving certification is only the beginning.

The Rule:

HITRUST requires ongoing:

- Risk management
- Security monitoring
- Policy enforcement
- Control validation
- Compliance reviews
- Continuous improvement

The Goal:

Build a compliance program that remains effective long after certification is achieved.

2. Understand Your Risk Environment

Effective compliance begins with understanding organizational risks.

Evaluate:

- Data protection risks
- Infrastructure vulnerabilities
- Third-party risks
- Access control weaknesses
- Operational threats
- Compliance gaps

The Red Flag:

If risks are only reviewed during audit preparation, compliance exposure increases significantly.

The Goal:

Identify and reduce risks before they affect security or compliance.

3. Build Strong Security Controls

HITRUST emphasizes comprehensive security governance.

Focus On:

- Access management
- Multi-factor authentication (MFA)
- Encryption standards
- Vulnerability management
- Security monitoring
- Incident response
- Data protection controls

The Bottom Line:

Strong security controls form the foundation of HITRUST compliance.

4. Documentation Matters

Incomplete documentation is one of the most common compliance challenges.

Maintain:

- Security policies
- Risk assessments
- Incident response plans
- Access management procedures
- Vendor management records
- Training documentation
- Audit evidence

The Goal:

Demonstrate readiness for compliance through clear and consistent documentation.

5. Access Control Must Be Managed Continuously

Access management is critical to protecting sensitive information.

Verify:

- User permissions
- Administrative access
- Remote access controls
- Account reviews
- Offboarding procedures
- Privileged account management

The Rule:

Users should have access only to the information necessary to perform their responsibilities.

6. Third-Party Risk Cannot Be Ignored

Vendors and service providers can introduce compliance and security risks.

Assess:

- Vendor security practices
- Data protection controls

- Compliance certifications
- Risk management processes
- Contractual obligations

The Goal:

Reduce exposure from third-party relationships.

7. Employee Awareness Strengthens Compliance

Technology alone cannot maintain compliance.

Train Teams On:

- Security awareness
- Data handling requirements
- Compliance responsibilities
- Phishing prevention
- Incident reporting
- Access management policies

The Bottom Line:

Well-trained employees help reduce compliance and security risks.

8. Prepare for Assessments Before They Happen

Organizations often struggle when preparing for audits at the last minute.

Maintain Audit Readiness:

Review:

- Control effectiveness
- Security documentation
- Risk assessments
- Policy updates
- Compliance evidence
- Remediation activities

The Goal:

Reduce audit stress and improve certification readiness.

9. Compliance Should Support Business Growth

Strong compliance programs improve more than audit outcomes.

Align HITRUST With:

- Risk management initiatives
- Customer trust objectives
- Security strategies
- Regulatory requirements
- Business continuity planning
- Operational resilience goals

The Goal:

Use compliance as a business advantage rather than an operational burden.

The Final Word

Stop treating HITRUST compliance as a certification project and start treating it as a long-term security and risk management strategy.

A mature HITRUST compliance program strengthens security, improves audit readiness, reduces risk, and demonstrates a commitment to protecting sensitive information and maintaining operational excellence.

Next Step:

Evaluate your current compliance posture today. Then determine whether your organization is building a sustainable HITRUST program or simply preparing for the next assessment.