RedHelm

ACTION GUIDE:

HOW TO MOVE FROM COMPLIANCE TO CONTINUOUS RISK MANAGEMENT

STEP 1:
Understand What Compliance Actually Proves

Identify which regulations, frameworks, contractual requirements, and cyber insurance obligations apply to the organization.
Document what each requires, but also recognize what those requirements do not prove about the organization's broader security posture.

STEP 2:
Connect Requirements to Real Business Risks

For each major compliance requirement or control, ask:

- What risk does this address?
- Which systems or data does it protect?
- What happens if this control fails?
- Who owns the control?
- How critical is it to business operations?

This transforms compliance requirements into meaningful risk management decisions.

STEP 3:
Validate That Controls Actually Work

Do not assume deployment equals effectiveness.

Regularly validate controls through:

- Vulnerability assessments
- Penetration testing
- Access reviews
- Backup and recovery testing
- Configuration reviews
- Security monitoring
- Incident response exercises

The objective is proving that controls function as intended.

RedHelm

STEP 4:
Monitor Changes Between Assessments

The environment that passed an assessment may not be the environment operating six months later.

Monitor changes involving:

- Users
- Privileged access
- Vulnerabilities
- Cloud environments
- Vendors
- Applications
- AI tools
- Security configurations

Continuous visibility helps prevent compliance drift.

STEP 5:
Make Cyber Risk an Ongoing Leadership Conversation

Cybersecurity compliance should feed executive-level conversations around:

- Business risk
- Investment priorities
- Operational resilience
- Cyber insurance
- Regulatory exposure
- Incident readiness
- Strategic technology decisions

The strongest programs use compliance findings to determine what should happen next.

Compliance is the starting point. Continuous risk management is the operating model.

Turn your incident response plan into a tested capability.

412.349.6680 www.redhelm.com