

COMPLIANCE & CYBER INSURANCE READINESS CHECKLIST



Executive Overview: Readiness Is No Longer Optional

Organizations are facing increasing pressure to demonstrate cybersecurity maturity; not just internally, but to regulators, insurers, and stakeholders.

Cyber insurance requirements are tightening. Compliance expectations are expanding. And executive accountability continues to grow.

This checklist provides a practical framework to help leadership teams evaluate whether their organization is prepared, and where gaps may exist.

As outlined in OXEN Assure & Compliance blog - Turning Risk Management into Business Confidence, modern organizations are expected not only to manage risk, but to prove they are doing so effectively.

Section 1: Visibility & Risk Awareness

Do you have clear visibility into your environment?

- ☐ Do you maintain an up-to-date inventory of systems, devices, and users?
- ☐ Do you have continuous visibility into vulnerabilities across your environment?
- ☐ Are you able to identify risky behavior or anomalous activity in real time?
- ☐ Do you understand which risks have the greatest business impact?

Executive Insight: You cannot manage, or insure, what you cannot see.

Section 2: Security Controls & Protection

Are your defenses aligned with modern requirements?

- ☐ Is multi-factor authentication (MFA) enforced across all critical systems?
- ☐ Do you have endpoint detection and response (EDR) in place?
- ☐ Is email security actively filtering phishing and malware threats?
- ☐ Are systems regularly patched and maintained?
- ☐ Do you have continuous monitoring and threat detection in place?

Executive Insight: Insurers expect controls to be active, enforced, and continuously validated.

Section 3: Policies & Documentation

Can you demonstrate control to auditors and insurers?

- ☐ Do you have documented cybersecurity policies and procedures?
- ☐ Are policies regularly reviewed and updated to reflect current risks?
- ☐ Can you produce documentation quickly for audits or insurance reviews?
- ☐ Do you have an incident response plan that is tested and maintained?

Executive Insight: Documentation is not optional; it is required proof of readiness.

Section 4: Continuous Validation & Testing

Are you validating your security posture consistently?

- ☐ Do you conduct regular vulnerability scanning?
- ☐ Are you continuously testing your environment for real-world exposure?
- ☐ Do you track remediation progress over time?
- ☐ Are results prioritized based on business impact; not just technical severity?
- ☐ Is security validation continuous rather than point-in-time?

Executive Insight: Security that isn't tested cannot be trusted.

Section 5: Compliance & Regulatory Alignment

Are you aligned with industry and regulatory expectations?

- ☐ Are your controls mapped to recognized frameworks (CIS, NIST, etc.)?
- ☐ Do you maintain ongoing compliance; not just audit readiness?
- ☐ Are roles and responsibilities clearly defined for compliance ownership?
- ☐ Can leadership confidently demonstrate due diligence?

Executive Insight: Compliance is no longer a periodic event; it is a continuous obligation.

Section 6: Cyber Insurance Readiness

Can you meet insurer expectations?

- ☐ Do you have evidence of continuous monitoring and response?
- ☐ Can you demonstrate how risks are identified and mitigated?
- ☐ Do you maintain documentation of security controls and validation?
- ☐ Are you prepared for underwriting review at any time?

Executive Insight: Failure to meet these requirements can result in increased premiums, or denied coverage.

Section 7: Executive Visibility & Reporting

Do leadership teams have the clarity they need?

- ☐ Do you receive clear, executive-level security reporting?
- ☐ Are risks translated into business impact; not just technical detail?
- ☐ Can you track improvement over time?
- ☐ Are cybersecurity decisions aligned with business priorities?

Executive Insight: If leadership cannot clearly understand risk, it cannot effectively manage it.

Scoring Your Readiness

Mostly “No”

Reactive approach

→ High exposure and audit risk

Mixed Answers

Transitional stage

→ Progress made, gaps remain

Mostly “Yes”

Mature security posture

→ Strong alignment with compliance and insurance expectations



Closing Perspective: From Compliance to Confidence

The goal is not simply to check boxes.

It is to create confidence:

- Confidence that systems are protected
- Confidence that requirements are being met
- Confidence that leadership understands and controls risk

As emphasized in the blog, **OXEN Assure & Compliance - Turning Risk Management into Business Confidence**, organizations must move beyond reactive compliance toward structured, continuous readiness.

Call to Action

Understand where you stand, and what to do next.

Use this checklist as a starting point to identify gaps, strengthen your security posture, and align your organization with modern compliance and cyber insurance expectations.

OXEN Technology

Strong. Simple. Trusted.®

888.296.3619 | hello@oxen.tech | OXEN.tech