Cloud Security and Governance Checklist:

IDENTIFY WHERE YOU ARE MOST AT RISK

The stakes for security teams have never been higher. Understanding how to uncover risks — and deploy mitigation strategies in your cloud environment are the first steps toward keeping your business safe from modern attacks.

Use the Onix Cloud Security Checklist for a high-level list of important factors to consider when assessing the security of your cloud environment. From security evaluation to enterprise security architecture and operations, our checklist can help you evaluate the security of your cloud-based environment and remediate findings.

Here's what to look for to Assess & Remediate:

Assess: Scan, Identify and Analyze Risks

Review cloud environment services and configurations.

- Generate security posture insights and data for analysis.
- Identify common misconfigurations and issues.
- Understand trends and problems that may exist based on the data collected.

Drill down on current issues reporting as “high” or “medium” issues/risks in different control domains.

1. POTENTIAL IAM FINDINGS.

- Organizational and account policy design challenges.
- Unused accounts and entitlements.
- Excessive privilege access that is used by individual user accounts.
- Password policy issues.

2. POTENTIAL INFRASTRUCTURE SECURITY GAPS.

- External ports open to ingress or egress access that are outside of normal risk tolerance.
- No observable use of VPC best practices.
- Misuse of VPC flow logs.
- Weak DDoS or WAF controls.
- Other foundational infrastructure security issues.

3. POTENTIAL LOGGING AND MONITORING EXCEPTIONS.

- Use of a centralized monitoring platform for alerts and health analytics.
- Disabled logging issues.
- Lack of log archives for long-term storage.
- Weak or ineffective log access controls.

4. POTENTIAL ENCRYPTION ISSUES:

- Identify where encryption is required but does not exist.
- KPM separation of duty weakness and issues.

Prioritize risks and develop a list of remediation activities in the risk register.

- Build and label risks to capture high and medium risks. Be sure to capture:
  - Risk level.
  - Issue type.
  - Date.
  - Remediation steps.
  - Due date.

Remediate Findings

Design, test, and implement controls based on a deep-dive review.

1. IAM REMEDIATION AND RECOMMENDATIONS:

- ✓ Remove unused user and service accounts.
- ✓ Remove or mitigate admin and privileged access from user accounts.
- ✓ Modify IAM to strengthen password policy requirements.
- ✓ Physically secure super admin account.
- ✓ Remove or mitigate personal email accounts where used.
- ✓ Resolve KMS user separation of duty issues.
- ✓ Modify controls that are not using service account least privilege best practices.

2. INFRASTRUCTURE SECURITY REMEDIATION AND RECOMMENDATIONS:

- ✓ Close ports to services that are deemed high risk.
- ✓ Implement VPC service controls for sensitive data.
- ✓ Enable VPC flow logs.
- ✓ Develop steps to deploy DDoS and WAF controls.

3. LOGGING AND MONITORING REMEDIATION AND RECOMMENDATIONS:

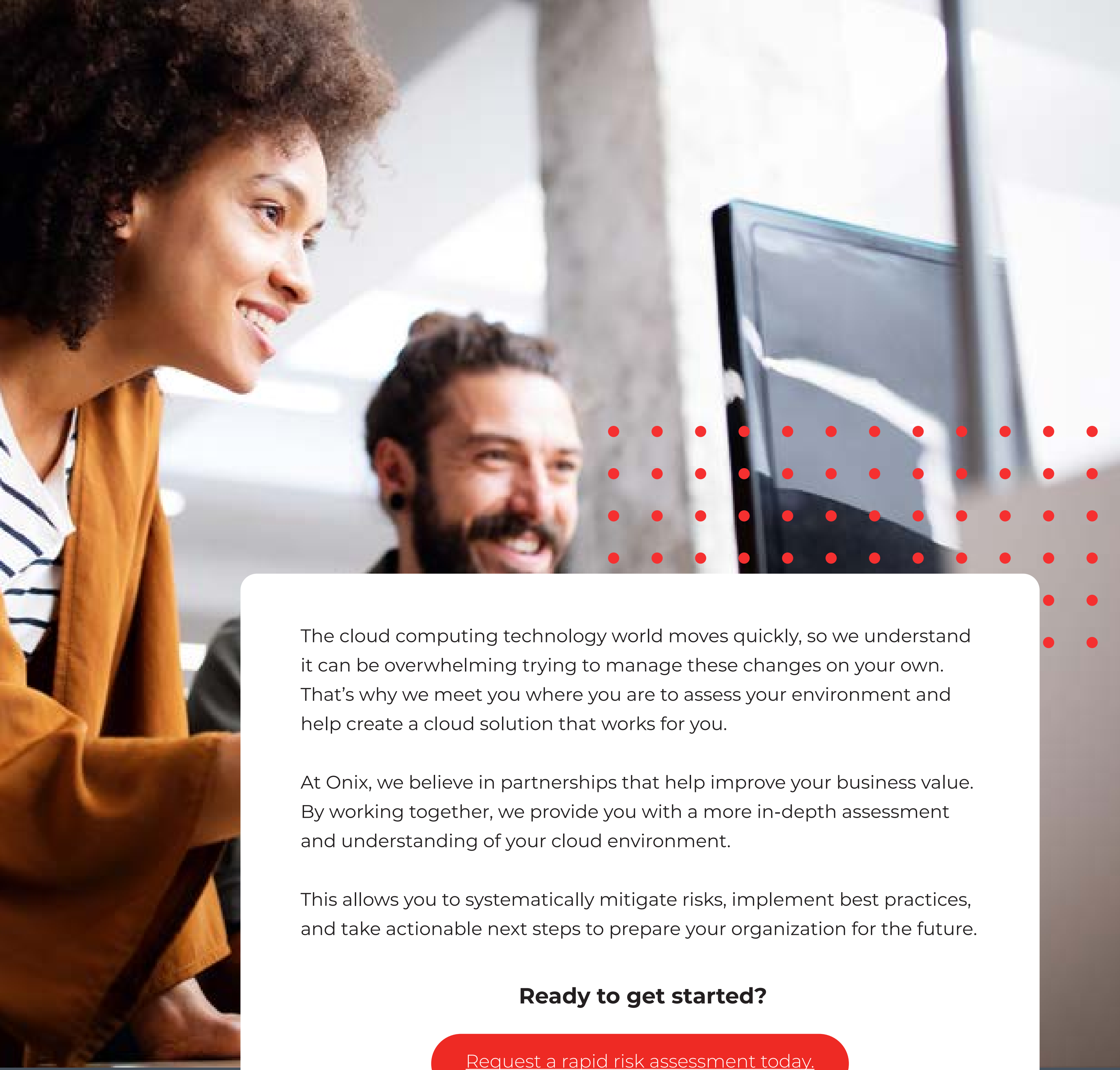
- ✓ Enable logging based on risks from scans.
- ✓ Configure storage for log data.
- ✓ Update logging access controls.

4. ENCRYPTION REMEDIATION AND RECOMMENDATIONS:

- ✓ Enable encryption based on data classification and risk.
- ✓ Where transmitted data is unencrypted, configure end-to-end transit encryption.

5. RE-SCAN FOR GAPS AND ISSUES:

- ✓ Make minor adjustments as needed to reach control effectiveness objectives.
- ✓ Close related risk register items.



The cloud computing technology world moves quickly, so we understand it can be overwhelming trying to manage these changes on your own. That's why we meet you where you are to assess your environment and help create a cloud solution that works for you.

At Onix, we believe in partnerships that help improve your business value. By working together, we provide you with a more in-depth assessment and understanding of your cloud environment.

This allows you to systematically mitigate risks, implement best practices, and take actionable next steps to prepare your organization for the future.

Ready to get started?

Request a rapid risk assessment today.