The Challenges of Getting Your Solution Security Approved

Janice Pearson SVP XL8

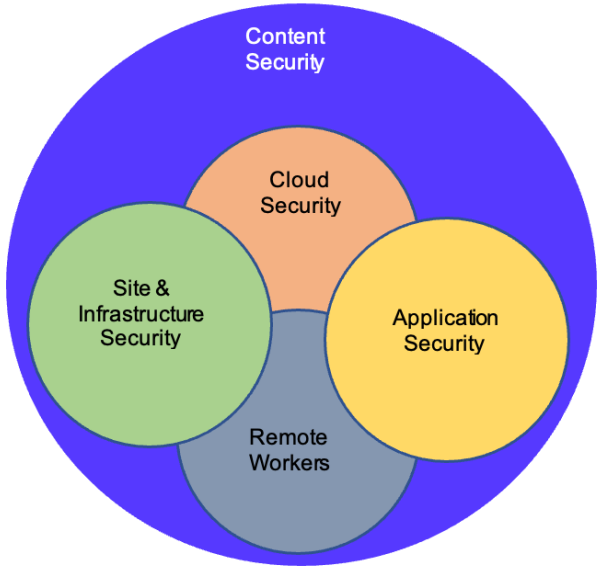
Chris Johnson CEO &Founder Convergent Risks

convergent

V1_04 – March 2022

Overview

- Get the environment right
- Embed cyber security into your business
- Grow your cyber security expertise
- Develop a positive cyber security culture



Dispel the Myths

convergent

Myth Busters:

With thanks to the UK's National Cyber Security Centre

- Myth #1: Cyber is complex, I won't understand it.
- Reality: You don't need to be a technical expert to make an informed cyber security decision.
- Myth #2: Cyber attacks are sophisticated, I can't do anything to stop them.
- Reality: Taking a methodical approach to cyber security and enacting relatively small changes can greatly reduce the risk to your organisation.
- Myth #3: Cyber-attacks are targeted, I'm not at risk.
- Reality: Many cyber-attacks are opportunistic and any organisation could be impacted by these untargeted attacks.

Get the environment right Take Away

convergent

1. Collate the information you sill need to make informed decisions about risk

- Collaborate with your clients suppliers and partners
- Establish the baseline that is right for your baseline and identify what you care about most
- Understand the cyber security threat

2. Use this information to evaluate and prioritise your activities.

- Assess what your risks are and understand the criticality

3.Take steps to manage those risks.

- Leverage a recognized security program
- Implement effective cyber security measures
- Plan your response to cyber incidents

Types of Assessments and Services relevant to M&E

convergent

Core Assessment Services

- Cloud Security Assessment
  - Including Cloud Configuration Vulnerability Testing
- Site & Infrastructure Assessment
- Application Service Provider (SaaS) Assessment
- Remote worker assessment

Required Security Testing as part of above

- External API & Web Application Penetration testing
- External Infrastructure Penetration testing
- Internal Security Assessment (Web & Infrastructure testing)
- Code review

Other Relevant Services

- OWASP ASVS Application Security Assessment (If external)
- Cloud Security Design Reviews
- Application Hardening Assessment
- Other Industry Standards Benchmarking (Can be reviewed as part of Core Assessment as there will be overlap)

convergent

10 Operational Domains	6 GRC Domains	4 Service Provider Domains
• Data Protection • Cryptography, Encryption Key and Secret Management • Network Security • Vulnerability Management • Patch Management • Anti-Malware • Logging and Monitoring • Pipeline • Hardening • Endpoint Protection	• Human Resources • Governance, Risk and Compliance • Incident Management • Change Control Management • Security Testing • Secure Coding	• Business Continuity Management and Operational Resilience • Audit and Assurance • Interoperability and Portability Policy and Procedures • Supply Chain Management, Transparency, and Accountability

convergent

Domain	Best Practice	Implementation Guidance	Evidence
Incident Management	Identify IR team & actions	IR policies & capability to assess, respond, learn, communicate	Reports & individuals
Logging and Monitoring	Ensure active solution (SIEM) is in place	Use AWS Guard Duty, Security Hub or 3rd party e.g., Splunk	Screenshot of tools
Patch Management	Deploy on virtual machines	Use AWS native or 3rd party solution	Show what tools are used?
Identity and Access Management	Ensure MFA is in place	Use AWS tools	Evidence for all cloud users
Vulnerability Management	Threat Modelling and Analysis	Description & processes	Show threat Modelling and Analysis process

convergent

Cloud Service Provider Best Practice + Cloud Security Alliance Cloud Control Matrix
Simplifying the complexity

Plus: Cloud Configuration Vulnerability Scanning

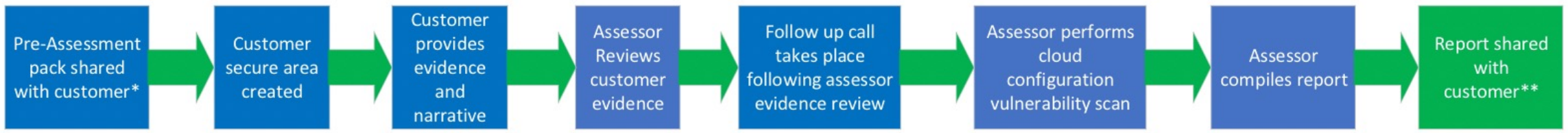
112 Controls & Best Practices

- 37 cloud service provider best practices sourced from AWS, GCP, Azure
- 64 sourced from CSA CCM controls v4
- 11 additional for SaaS Service Providers sourced from CSA CCM controls v4.05

Subject to use case

- Cloud service consumers (64 + 37) = 101 controls
- SaaS Application Service Providers (64 + 37 + 11) = 112 controls
- Hybrid Vendors – add relevant MPAv4.09/TPN best practices

- Initial call to explain process
- Scope relevant workflow
  - Review cloud architecture, qty of cloud accounts, status of threat assessment pen testing via scoping form
- Pricing for approval
- Best practice questionnaire made available & completed by vendor
- Assessor completes assessment
- Draft report made available to vendor
- Final report submitted to the vendor
- Remediation management



Timing

Day 1

Kick off

Questionnaire made available

Day 30

Questionnaire complete with evidence

Configuration Testing

Threat assessment reviewed or actioned

Day 40

Assessment takes place

Clarification & questions

Report Produced

Reporting

- Executive Summary
- Detailed Report
- Description of Best Practice
- Identification of vulnerabilities
- Reason for vulnerability
- Advice and guidance on remediation

convergent

Thank You for your attention

convergent

Questions?