



CONTINUOUS MONITORING

THE WHOLE PICTURE

Sr. Federal Solutions Engineer

David Pricer

David.Pricer@verizon.com

4.2.2015

PTEXXXX XX/14

Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.



Continuous Monitoring The Whole Picture

- Introduction
- GRC
- Continuous Monitoring
- Process, People & Technology
- Recommendations Review
- Questions



Continuous Monitoring The GRC Discussion

Compliance: is either a state of being in accordance with established guidelines or the process of becoming so – *COSO ERM*



Risk: a positive or negative event. – *ISO 31000*

Governance: a combination of external factors which affect the way a corporation is operated. – *COSO ERM*

Continuous Monitoring Industry's Thought

- Vulnerability Scanning
- Mention the Risk Management Framework or NIST SP800-137
- Collection of Data
- Direction of Compliance
- Make it SCARY!





Continuous Monitoring Defined

- FISMA
- Risk Management Framework
 - NIST SP800-37
 - Risk Management may be viewed as a holistic activity that is fully integrated into every aspect of the organization.
 - NIST SP800-137
 - Any effort or process intended to support ongoing monitoring of information security across an organization begins with leadership defining a comprehensive ISCM strategy encompassing technology, processes, procedures, operating environments, and people.
 - FedRAMP
 - DHS CDM – Continuous Diagnostics & Mitigation





Continuous Monitoring Process

- How to Boil the Ocean in 3 Easy Steps
- Threats/Vulnerabilities, (Risks)
 - Process & Policy Management
 - System Development Life Cycle



- Threats/Vulnerabilities (Risks)
 - Social Engineering
 - Verizon DBIR
 - Stolen Credentials
 - Phishing
 - Brute Force
 - User Behavior
 - Corporate Culture
 - Proactive RM vs. Reactive Compliance
 - Operational Security ... Not Operations & Security
 - Performance Measurement
 - Executive Buy-In with TEETH!





Continuous Monitoring Technology

- Threats/Vulnerabilities, (Risks)
 - Budget, Technology, Compliance
- Advanced Persistent Threats (YOU WILL BE BREACHED!)
 - Anthem, Sony, Home Depot, Target
 - Your budget is not the solution



Continuous Monitoring Recommendations Review

- Organizational Gap Assessments
- Well defined Corporate Objectives
- Corporate Culture
- Technology Due Diligence
- Performance Measurement/BI
- Understand Maturity Levels
- Use Continuous Monitoring as it is meant to be by ensuring an organizational wide view to feed metrics to the risk management process





Questions?





- FISMA
- Risk Management Framework (RMF)
- NIST SP800-137 – Continuous Monitoring
- NIST SP800-37 – Applying the RMF
- FedRAMP Website: <https://cloud.cio.gov/>