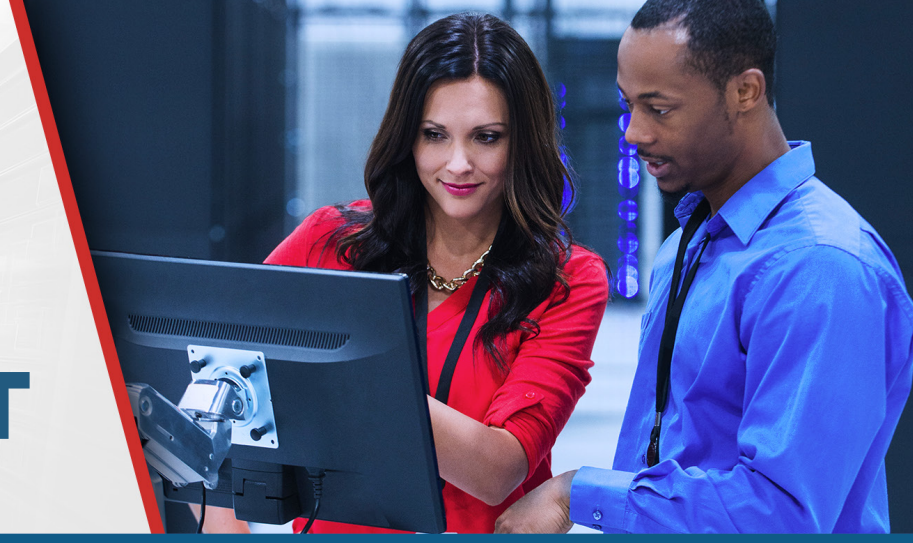
PCM THE RIGHT TECHNOLOGY, DELIVERED

SECURITY PROGRAM ASSESSMENT



DOES YOUR SECURITY PROGRAM MANAGEMENT ADD UP?

Your security threat matrix is always changing. Each change in business process, model, technology and organizational structure brings new risks to your security posture and mission-critical data. The PCM Security Program Assessment (SPA) is designed to assess your current security management program against the evolving threat matrix. The SPA is not a penetration or vulnerability assessment. The SPA is based on ISO /ISE 2700x that measures the maturity of a client's Information Security Management Program (ISMP).

How do you determine if your security posture is sufficiently mature?

TWO SIMPLE QUESTIONS

1. Have you looked at your security management program and assessed whether it is ready to defend against the latest threats such as Wannacry, Krack, and Blueborne?
2. Has your security management program kept up with your changing data processing environment such as mobile, trusted third party access, cloud access, SSL encryption traffic?

If the answer is "no" or "not sure" to either of those questions, your organization should take the time to accurately assess its current risk level and security needs.

A Wakeup Call

A Security Program Assessment (SPA) is often used as a wakeup call for executive management by exposing security risks that can lead to financial and reputational loss, and to secure the resources necessary to support a security posture commensurate with your organization's risk tolerance.

When doing a Security Program Assessment, we identify deficiencies with the organizational Information Security Management Program that leads to systemic vulnerabilities.

SECURITY PROGRAM ASSESSMENT

The SPA will identify weaknesses in the Security Program such as the lack of a viable Patch Management Program, or a flawed Change Management Procedure that lead to vulnerabilities. During a SPA we will assess such things as:

- **Business Drivers & Challenges**
- **Risk Appetite**
  - Risk Mitigation
  - Risk Acceptance
  - Risk Avoidance
  - Risk Transference
- **Enterprise Risk Posture**
- **Data Sensitivity & Classification**
- **Current security technologies deployed**
- **Business Risk Impact**
- **Security – Compliance – Privacy**

- **Assess the following ISO27002/ISMP Domains as they relate to the 7 Domains of a Typical IT Infrastructure Framework:**
  - Risk Assessment & Treatment
  - Security Policy
  - Organizational Policy
  - Asset Management
  - Human Resources Management
  - Physical and Environmental Security
  - Communication and Operations Management
  - Access controls
  - IS Acquisition, Development and Maintenance
  - Incident Event & Communications Management
  - Business Continuity & Disaster Recovery Management
  - Compliance Management
  - Mobile Security
  - Privacy
  - Software Application Security
  - Cloud Security

Security as a Profit Center

A mature security posture—one that encompasses people, processes and technology—can change your security program from a cost center to a business enabler. Our SPA will provide for a Security Program that offers a practical security approach that enables you to meet your business goals. In addition, the cost efficiencies gained from risk mitigation, fraud prevention, operating efficiencies, data protection and brand reputation can be quantified and verified.

To that end, it is critical to work with highly experienced security professionals with a deep and broad understanding of IT security in a business context. It doesn't matter how advanced your security program is or whether you need to assess the security posture of a strategic business unit, subsidiary or the entire enterprise. Every SPA is customized to align with your business objectives and operating procedures, because it is not enough to be compliant. You must be secure.