Professional Security Services Modules List

Date:
As at March 2013

Executive Summary

Introduction

About IPSec

IPSec are specialists in information asset security; technology experts who know how to mitigate risk to business by implementing end-to-end solutions that protect invaluable intelligence, data and information. From assessing vulnerabilities and threats, to designing and implementing customised security strategies, to managing execution and optimising results. IPSec are guardians of business confidence, providing high levels of protection and optimal assurance of an organisation's security posture.

IPSec is about mitigating risk; enabling confidence and agility by ensuring a reliable IT environment that allows business to get on with business.

Introduction to IPSec Professional Security Services

IPSec's Professional Security Services (PSS) represent a complete suite of IT security engineering and IT security consulting services. IPSec's modular approach to PSS enables a quick and precise response to any security problem in a highly cost-predictable and scalable manner.

IPSec can assist in reviewing existing security postures, the deployment of security solutions, or assessment of the best path to an improved security outcome.

This document provides a high level listing of IPSec predefined security methodologies for discussion.

Available PSS Modules

The following is a list in brief of the more common IPSec services methodologies. Please contact IPSec for discussion around appropriate modules and scope.

- **Modules for Firewalls, VPNs, TM, IDS' and IDP/IPS'**
  - PSSM1.1 – Firewall, VPN, TM, IDS and/or IDP/IPS Deployment
  - PSSM1.2 – Firewall, VPN, TM, IDS and/or IDP/IPS Adjustment
  - PSSM1.3 – Firewall, VPN, TM, IDS and/or IDP/IPS Configuration Review
  - PSSM1.4 – Firewall, VPN, TM, IDS and/or IDP/IPS Performance Review
- **Modules for Anti-Virus Solutions**
  - PSSM2.1 – Anti-Virus Solution Deployment
  - PSSM2.2 – Ant-Virus Solution Adjustment
  - PSSM2.3 – Anti-Virus Solution Configuration Review
  - PSSM2.4 – Anti-Virus Solution Performance Review
- **Modules for Content Management Solutions**
  - PSSM3.1 – Content Management Solution Deployment
  - PSSM3.2 – Content Management Solution Adjustment
  - PSSM3.3 – Content Management Configuration Review
  - PSSM3.4 – Content Management Performance Review
- **Modules for Authentication Solutions**
  - PSSM4.1 – Authentication Solution Deployment
  - PSSM4.2 – Authentication Solution Adjustment
  - PSSM4.3 – Authentication Configuration Review
  - PSSM4.4 – Authentication Performance Review
- **Modules for Security Strategy**
  - PSSM5.1 – Security Strategy Workshop
  - PSSM5.2 – Security Strategic Planning
  - PSSM5.3 – Security Strategic Plan Review
- **Modules for Security Policy & Procedure**
  - PSSM6.0 – Custom Policy and/or Procedure Requirement (as specified).
  - PSSM6.1 – Security Policy and/or Procedure Development
  - PSSM6.2 – Security Policy and/or Procedure Education
  - PSSM6.3 – Security Policy and/or Procedure Review
  - PSSM6.4 – AS/NZS ISO/IEC 27001 & 27002 Alignment
  - PSSM6.4.1 – Information Security Ownership
  - PSSM6.4.2 – Third Party Access Control & Data Exchange
  - PSSM6.4.3 – Third Party Service Contract Review
  - PSSM6.4.4 – Asset Identification & Classification
  - PSSM6.4.5 – Asset Classification Rules Definition
  - PSSM6.4.6 – Employee Security
  - PSSM6.4.7 – Physical Environment Security
  - PSSM6.4.8 – Physical Equipment Security
  - PSSM6.4.9 – Secure Change Control
  - PSSM6.4.10 – Security Incident Identification
  - PSSM6.4.11 – Security Incident Management
  - PSSM6.4.12 – Data Handling & Disposal
  - PSSM6.4.13 – User Access Review

- PSSM6.4.14 – Endpoint Access Control
- PSSM6.4.15 – Sensitive System Identification & Control

- **Modules for Network Services Security**
  - PSSM7.1 – Network Services Identification
  - PSSM7.2 – Network Services Volume Vulnerability Identification
  - PSSM7.3 – Network Services Zero-Day Vulnerability Identification
  - PSSM7.4 – Internal Penetration Test
- **Modules for Application Security**
  - PSSM8.1 – Website CGI Assessment (Non-Authenticated Users)
  - PSSM8.2 – Website CGI Assessment (Authenticated Users)
  - PSSM8.3 – Website CGI Architecture
  - PSSM8.4 – Application Architecture
  - PSSM8.5 – Application Assessment (Non-Authenticated User)
  - PSSM8.6 – Application Assessment (Authenticated User)
- **Modules for Wireless Security**
  - PSSM9.1 – Active WiFi (802.11) Access Point Identification and Assessment
  - PSSM9.2 – Active Bluetooth Device Identification and Assessment
- **Modules for Network Security**
  - PSSM10.1 – Network Architecture Security Design
  - PSSM10.2 – Network Architecture Security Review
  - PSSM10.3 – Network Traffic Review
  - PSSM10.4 – Network Access/Admission Control Deployment
- **Modules for Desktop & Server Security**
  - PSSM11.1 – Desktop SOE Security Review
  - PSSM11.2 – Server General and/or SOE Security Review
  - PSSM11.3 – Mobile Device SOE Security Review
  - PSSM11.4 – Directory Controlled User Permissions Review
  - PSSM11.5 – Database Server Assessment
- **Modules for Data Leakage Protection**
  - PSSM12.1 – Data Leakage Protection Review
  - PSSM12.2 – Data Leakage Protection Deployment
  - PSSM12.3 – Data Encryption Deployment
  - PSSM12.4 – Data Encryption Adjustment
  - PSSM12.5 – Data Encryption Configuration Review
  - PSSM12.6 – Data Encryption Performance Review