

Axean Pacific Security Readiness Assessments

Partial Areas of Coverage

The following list represents a portion the areas typically covered in a Security Readiness Assessment. Each Assessment, however, is tailored to meet the client's individual requirements.

1. Introduction

- 1.1. Purpose
- 1.2. Goals
- 1.3. Methods
- 1.4. Role of Axean Pacific

2. Summary of Findings and Recommendations

3. [CUSTOMER] Business Drivers

- 3.1. [CUSTOMER] Overview
 - 3.1.1. Key [CUSTOMER] personnel
 - 3.1.1.1. CIO/CTO
 - 3.1.1.2. CSO
 - 3.1.1.3. Others
- 3.2. Business Priorities and Strategies
- 3.3. Compliance requirements
- 3.4. Partners and Suppliers

4. [CUSTOMER] Information Technology Summary

- 4.1. Corporate Information Systems
- 4.2. Current Projects
- 4.3. Current Information Systems Infrastructure

5. Security Assessment

- 5.1. Threat Analysis
 - 5.1.1. Internal Threats
 - 5.1.2. External Threats
 - 5.1.3. Risk Assessment

5.2. Inventory Results Summary

5.3. Vulnerability Assessment

5.3.1. Authentication

5.3.2. Authorization

5.3.3. Organizational Assessment

5.3.4. Policies

5.3.5. Network Physical Design

5.3.6. Network Logical Design

5.3.7. Servers

5.3.8. Network Vulnerability Assessment

5.3.9. Active Content Monitoring/Filtering and Virus Detection

5.3.10. Intrusion Detection

5.3.10.1. Host Based

5.3.10.2. Network Based

5.3.11. Data Protection

5.3.12. Disaster Preparedness

5.3.13. Logging

5.3.14. Remote Access/Back Door Analysis

5.3.15. System Testing

5.3.16. Support Architecture

5.3.17. Web and Internet Systems

5.3.18. Databases and Applications

5.3.19. Databases

5.3.20. Encryption

5.3.21. Incident Response

5.4. Penetration Testing

6. Security Gap Analysis

6.1. Gaps Identified

6.2. Prioritization of Information Assets

6.3. Gap Prioritization

7. Threat Reduction Plan

- 7.1. Threat Reduction Strategy
 - 7.1.1. Defense-In-Depth
 - 7.1.2. Isolation
 - 7.1.3. Defense Maintenance
 - 7.1.3.1. Policy Review
 - 7.1.3.2. Enforcement
 - 7.1.3.3. Network Assessment
 - 7.1.3.4. Intrusion Detection
 - 7.1.3.5. Data and Systems Maintenance
 - 7.1.3.6. Application Vulnerability Assessment
 - 7.1.3.7. Security in Design
 - 7.1.3.8. Model Office Laboratory Security Implementation
 - 7.1.4. Configuration Management
 - 7.1.5. Threat Assessment Planning and Prioritization
- 7.2. Immediate Actions Required
- 7.3. Short-term Actions Recommended
- 7.4. Moderate-term Actions Recommended
- 7.5. Long-term Actions Recommended