

# **A PRACTICAL GUIDE TO SECURITY ASSESSMENTS**

## **INTRODUCTION**

### **EVOLUTION OF INFORMATION SECURITY**

- Distributed Systems
- Business-to-Business (B2B) Relationships
- Remote Access
- Enterprise Resource Planning (ERP)
- Information Security Today
- Why Protect Information Assets
- Growing Role of Internal Audit
- Security Standards
- Organizational Impacts
- Security Certifications
- Trends in Information Security

### **INFORMATION SECURITY PROGRAM AND HOW SECURITY ASSESSMENTS FIT IN**

- What is an Information Security Program
- How Does a Security Assessment Fit In
- Why Conduct a Security Assessment
- Security Assessment Process
- Executive Summary

### **PLANNING**

- Define Scope
- Staffing
- Kickoff Meeting
- Develop Project Plan
- Set Client Expectations
- Executive Summary

### **INITIAL INFORMATION GATHERING**

- Gather Publicly Available Information
- Gather Information from the Client
- Analyze Gathered Information
- Prepare Initial Question Sets
- Develop and Document Template for Final Report
- Executive Summary

### **BUSINESS PROCESS EVALUATION**

- General Review of Company and Key Business Processes
- Finalize Question Sets for Process Reviews
- Meet with Business Process Owners
- Analyze Information Collected and Document Findings
- Status Meeting with Client
- Potential Concerns During This Phase
- Executive Summary

### **TECHNOLOGY EVALUATION**

- General Review of Technology and Related Documentation
- Develop Question Sets for Technology Reviews
- Meet with Technology Owners and Conduct Detail Testing

**BUY ONLINE AT: <http://www.27001.com/products/86>**

Analyze Information Collected and Document Findings  
Status Meeting with Client  
Potential Concerns During this Phase  
Executive Summary

### **RISK ANALYSIS AND FINAL PRESENTATION**

Risk Analysis  
Risk Score Calculation  
Document Risks and Develop Recommendations for Draft Report  
Discuss Draft Report with Client  
Present Final Report to Management  
Potential Concerns During this Phase  
Executive Summary

### **INFORMATION SECURITY STANDARDS**

International Standards Organization 17799 (ISO 17799)  
Common Criteria (CC)  
COBIT (Control Objectives for Information (Related) Technology)  
ITIL (IT Infrastructure Library) Security Management  
SAS (Statement on Auditing Standards) 70  
AICPA SysTrust  
AICPA WebTrust  
RFC 2196 - Site Security Handbook  
SANS (SysAdmin, Audit, Network, Security) / FBI Top 20 List  
Vendor Best Practices

### **INFORMATION SECURITY LEGISLATION**

Relevance to Security Assessments  
HIPAA (Health Insurance Portability and Accountability Act)  
GLB Act (Gramm-Leach-Bliley Act)  
Sarbanes - Oxley Act  
21 CFR Part 11  
Safe Harbor  
Federal Information Security Management Act  
Other Legislative Action

### **APPENDIX - SECURITY QUESTIONNAIRES/ CHECKLISTS**

Questionnaire Structure  
Preliminary Checklist to Gather Information  
Generic Questionnaire for Business Process Owners  
Data Classification  
Data Retention  
Backup and Recovery  
Externally Hosted Services  
Physical Security  
Employee Termination  
Incident Handling  
Business to Business (B2B)  
Business to Consumer (B2C)  
Change Management  
User ID Administration  
Managed Security  
Media Handling  
HIPAA Security