



Business Security Assessments

What every executive needs to know
before selecting a security evaluation

An Informatica Security White Paper
October 2004

Author:
Claudiu Popa, President
Informatica Corporation



TABLE OF CONTENTS

Introduction	3
Examples For Each Assessment Type	4
Assessment Type Options	4
Selecting The Right Assessment	5

Informatica Corporation provides corporations with information security consulting, services and technology. With expertise spanning 15 years, Informatica is a recognized industry innovator and corporate advisor. Services include executive consulting, security management, complete training programs, risk management, management support and industry-leading security assessments. (www.InformaticaSecurity.com)

Copyrights and trademarks of Informatica Corporation include: FlexSecure Verify (audits, analysis and assessments), FlexSecure LockDown (secure systems), FlexSecure DataScrub (secure data destruction), FlexProtect (corporate security support) and FlexProtect SM (security management), WorkLife Learning (corporate training).

Introduction

Businesses of all sizes, non-profit organizations and governments are operating in an environment where information has not only become a valuable business asset but it is defining the value of the organization. Every executive needs to be conscious of the risk to information assets and have a plan to mitigate that risk. The first step and a recurring element of every risk management strategy is the security assessment.

Informatica Corporation offers security assessments designed to provide managers, executives and business owners with the visibility they require to make informed decisions.

Business Security Assessments fall into 3 Categories:

1. Technical
2. Procedural
3. Business

Each Category is divided into two assessment types:

1. Technical

- a. Applications & Databases
- b Systems and Technology

2. Procedural

- c. Processes and Policies
- d. Standards & Regulatory Compliance

3. Business

- e. Overall Enterprise Risk
- f. Third Party Assessments

Security Assessments must be used to determine the impact of changes and situations on business goals and operations. Each type of assessment provides valuable insight into the risk associated with changes and events.

Examples For Each Assessment Type

ASSESSMENT TYPE	EXAMPLE
APPLICATIONS & DATABASES	Before investing in a new software product, venture capital firms need to conduct a thorough security assessment to avoid security risks and reduce the likelihood of security weaknesses. Database backed systems, especially online ecommerce sites need to be thoroughly reviewed for flaws that can compromise customer data and financial records.
SYSTEMS AND TECHNOLOGY	Networks, email and DNS systems need to be audited for internal and external vulnerabilities.
PROCESSES AND POLICIES	Business processes must incorporate security safeguards and procedures to preserve the overall security of business assets.
STANDARDS & REGULATORY COMPLIANCE	Compliance with internal policies, industry standards, third party requirements and legal regulations make recurring compliance audits a necessity.
OVERALL ENTERPRISE RISK	Insurance policies require overall enterprise risk evaluations. Mergers and Acquisitions require Enterprise or Divisional Risk Assessments.
THIRD PARTY ASSESSMENTS	Outsourcing Relationships, partnerships and collaborations require joint understanding of risks and procedures.

Each Security Assessment Type has many facets and is designed to precisely meet the requirements for risk identification, analysis, visibility and budgeting. These facets are provided as options with each engagement.

Assessment Type Options

a. Applications & Databases
1. Source code analysis
2. Penetration testing
3. Web site security audit
4. Database access and integrity
5. Web application vulnerability
6. Transactional integrity
7. Overall E-commerce system security

8. Hosting infrastructure
9. Communications integrity and confidentiality
10. Privacy compliance
11. Change management

b. Systems and Technology
1. Networking and Wireless Systems
2. Storage systems
3. Email and FTP (data transfer systems)
4. Network appliances and connected technology
5. Other hardware: banking ATMs, manufacturing PLCs, etc.
6. Ethical hacking
7. Zero knowledge analysis (black box)
8. Full knowledge analysis (crystal box)
9. Desktop security
10. Compliance integration and deployment
11. Remote access
12. Critical Systems Risk

c. Processes and Policies
1. Business process mapping and analysis
2. Policy compliance audits
3. Procedures and best practices awareness
4. Advanced: social engineering audit
5. Security effectiveness and reporting relationships
6. New Process assessment/integration

d. Standards & Regulatory Compliance
1. Risk management standards
2. Information security standards
3. Privacy standards

4. Regulatory (financial records protection) standards
5. Controls and effectiveness

e. Overall Enterprise Risk
1. Critical Systems Risk (management perspective)
2. Business Continuity
3. Enterprise Risk Management
4. Risk modelling and simulation
5. Mergers/Acquisitions
6. Human Resources/Hiring Practices
7. Corporate security awareness and communications

f. Third Party Assessments
1. Privacy and confidentiality compliance
2. Security policy compliance
3. Transactional and other financial operations
4. Technical controls and vulnerabilities
5. HR, Awareness and management education

Choosing The Right Security Assessment For Your Needs

Selecting the right assessment is a matter of knowing where you are in the risk management process. If your organization is just starting on the path to protecting information assets, then an enterprise audit is probably needed. Otherwise, a selection can be made based on the current situation and change management plans. Similarly, duration and pricing are dependent on every situation.

FlexSecure *Verify* services are non-intrusive security assessments conducted by experienced Informatica professionals according to standard risk management methodologies. These assessments are 50% more effective than traditional security assessments. Choose *Verify* to discover and start eliminating the risk.

www.SecurityAudits.ca