

# Control Essentials

Volume III, Issue VI

June 2008

**IT Security:**

Information security design and Implementation  
Vulnerability Assessments  
Penetration Testing  
Security Breach Investigation and Remediation  
Business Continuity Planning  
Logwatch  
Training

**Risk Management:**

Risk Assessment  
IT Risk Advisory  
Fraud Detection

**Forensic Services:**

Computer Forensics  
E-Discovery

**IT Audit Services:**

Application and System Implementation Reviews  
Internal Information Systems Audits

**Regulatory Compliance:**

Bank Secrecy Act  
Gramm-Leach-Bliley Act  
Fair and Accurate Credit Transactions Act  
Sarbanes-Oxley Act  
Health Insurance Portability and Accountability Act  
Family Educational Rights and Privacy Act  
Payment Card Industry

**Attestation Services:**

SAS 70 Reviews  
Other Attestation Services

## Security Risk Assessment Methodology

As security and privacy regulations increase, today's business environment is left with the daunting task of being proactive in managing risks. The best way to ensure that a business is fully aware of its current security status and keeps a watchful eye on potential security problems is to perform periodic security risk assessments.

Security risk assessments can help identify reasonably foreseeable external and internal threats, assess the likelihood and potential damage of these threats and assess the sufficiency of security controls in place to control risks.



The success of a security risk assessment boils down to the ability to develop a methodical and thorough approach to determine the levels of exposure of information systems and data to external and internal threats. Therefore, the most effective way to perform a comprehensive security risk assessment is to follow a structured methodology.

The selected methodology should identify, analyze and prioritize security risks that could compromise the confidentiality, integrity and availability of data. Additionally, the methodology should identify existing controls, inadequate controls and controls that are missing altogether.

The following sections summarize one of the methodologies that can be used. The said methodology covers the processes of identifying the organization's assets, classifying them in terms of sensitivity, identifying threats that impact them and the security controls in place to mitigate those threats.



### **Phase 1: Inventory of Information Assets**

The main objective of this phase is to identify information assets such as applications, electronic documents and physical documents that are used by the business to carry out its operations. During the inventory phase, sufficient information about the assets being inventoried should be collected as this phase will serve as the basis for the remaining phases. The information collected about the assets should include the name, type (application, physical document or electronic document) and area/department responsible for the asset as well as a description of the asset and the physical or logical location of the asset.

### **Phase 2: Classification of Information Assets**

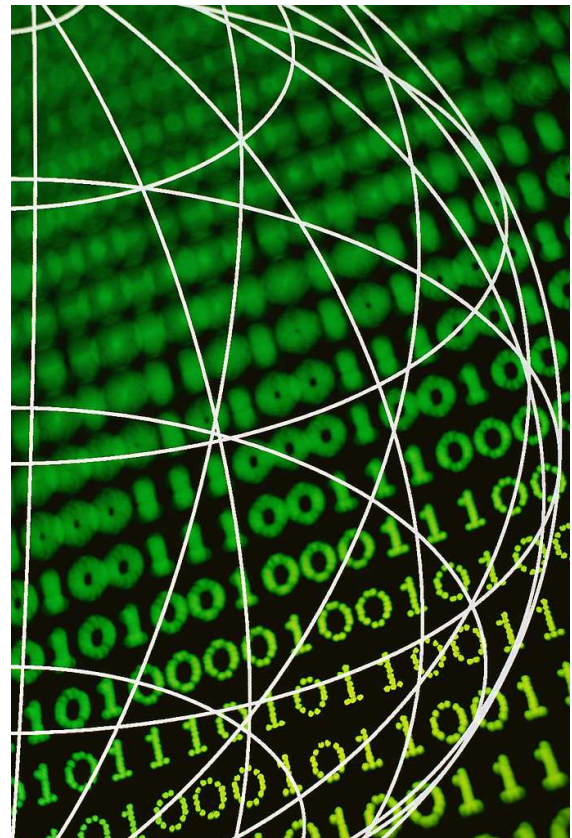
The main objective of this phase is to classify all the assets identified and inventoried according to the organization's information classification scheme. The classification scheme used should provide a method to rank assets in terms of sensitivity. After the assets are assigned a classification, each asset must be evaluated in terms of three primary security components: confidentiality, integrity and availability.

### **Phase 3: Threat Analysis**

The main objective of this phase is to identify major existing threats that affect the information assets of the business. The threats can range from malicious programs, disgruntled employees and alteration of data to natural disasters, electrical disturbances and vandalism. Each information asset must be evaluated in relation to the defined threats. For each threat, a value must be assigned to the probability that the threat will materialize and another value to the level of impact that would be incurred by the asset if the threat were to materialize. The main product of this phase is the determination of a final risk factor for each information asset. The final risk factor is a combination of the classification level, threat probability and impact which will be used to prioritize assets in accordance to risk levels.

### **Phase 4: Security Control Analysis**

The fourth and final phase of the security risk assessment process is intended to identify existing security controls for each individual information asset and detect any additional controls that should be in place. This phase should address the detailed testing of logical, physical and administrative security measures. Ideally, a mapping should be defined delineating the controls that would minimize each threat. For example, the threat of a hurricane could be minimized if adequate controls were in place for backup, recovery plan and physical security. The main purpose of this phase is to ensure that all the assets found to have the highest final risk factors in the previous phase have adequate and proper security controls in place.



## **Gap Analysis**

For a business to get the full benefit of a security risk assessment, a gap analysis should be performed upon completion of all four phases. A gap analysis identifies the security controls either currently missing or currently not working adequately in the control structure. By analyzing these control deficiencies, a business can document residual risk and decide whether to accept, mitigate or remediate the risks identified. In performing this task, a business must ensure that logical and justifiable reasoning is used to accept risks. This gap analysis should result in security control implementation plans organizing activities in order of priority for the organization.

## **Conclusion**

Once a working methodology is in place, there are a few key points to keep in mind in order to keep a proactive approach to security risk management. Security risk assessments should be performed on a regular basis. As the organization, processes, infrastructure, systems and data change, security risk assessments need to be conducted again to identify new risks. Lastly, the security risk assessment process is an on-going process. Just because significant changes have not taken place, it does not mean that the controls are still operating efficiently or that new threats are not present. Keep in mind that there is no silver bullet for a business's control structure. Security controls can always be fine tuned and optimized; hence taking a proactive active stance to risk management is the most effective way to secure your business.

*Best Boutique Risk Management Firm in South Florida.*

### **SOUTH FLORIDA CEO MAGAZINE, 2006**

*They have the ability to understand the needs of our organization and work well with our employees.*

### **THE INTERNATIONAL BANK OF MIAMI**

*We selected ERM because of their professional references, experience and reasonable professional fees.*

### **R G PREMIER BANK OF PUERTO RICO**

*ERM accomplished and exceeded objectives planned*

### **BACARDI - MARTINI, INC.**

## KEEPING WATCH OVER YOUR BEST BUSINESS INTERESTS

ERM professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" consulting firms to major corporations and prestigious professional certifications. A snapshot of ERM's profile can be seen below:

### Education

#### Qualifications

M. S. in Computer Information Systems  
M. S. in Information Networking  
M. S. in Management Information Systems  
Master of Accounting Information Systems  
Master of Business Administration

#### Universities

Carnegie Mellon University  
Syracuse University  
Xavier University  
University of Miami  
Florida International University

### Certifications

Certified Public Accountant (CPA)  
Certified Information Systems Security Professional (CISSP)  
Certified Information Systems Auditor (CISA)  
Certified Information Systems Manager (CISM)  
Certified Information Technology Professional (CITP)  
GIAC Security Essentials Certification  
GIAC Systems and Network Auditor  
Microsoft Certified Professional

### Prior Work Experience

PriceWaterhouse Coopers  
Deloitte  
CERT® Coordination Center  
SONY Electronics Latin America, Inc.  
RJR Nabisco  
Diageo plc  
Arthur Young  
Carnegie Mellon CyLab  
Evertec Inc.  
American Bankers Insurance Group  
Chesebrough Pond's  
Starboard Cruise Services, Inc.

### Some of our Clients...

ABN AMRO Private Banking  
Bacardi-Martini, Inc.  
Carnival Cruise Lines  
CitiBank  
Commerce Bank  
Florida Power & Light Company  
Knight Ridder  
North Broward Hospital District  
Ocean Bank  
Rinker Materials  
Sylvania Lighting International  
The International Bank of Miami

**enterprise risk management**

*The Control Professionals*

800 S. Douglas Road, North Tower # 835,  
Coral Gables, FL 33134.

P: (305) 447 6750 F: (305) 447 6752

Email: [info@emrisk.com](mailto:info@emrisk.com) Web: [www.emrisk.com](http://www.emrisk.com)