



Effectively Managing Information Security Risk

A guide for executives

Stan Stahl, Ph.D., President, Citadel Information Group
Kimberly A. Pease, CISSP, Vice President, Citadel Information Group

January, 2007

© Copyright 2007. Citadel Information Group, Inc. All rights reserved.

Table of Contents

Purpose of this White Paper.....	3
The Information Security Management Program	3
Information Security Management Program Objectives	4
Evolving Requirements for an Information Security Management Program	5
Managing the Security of Critical Information Assets	6
Information Security Control Objectives.....	6
Defense-in-Depth with Feedback	7
The Fundamental Equation of Information Security	7
Countermeasure Control Classes	8
Information Security Critical Success Factors.....	8
Management Control Domains	9
Managing the Information Security Program	11
Chief Information Security Officer (CISO).....	11
Information Security Steering Committee	11
Information Security Responsibilities.....	12
Creating an Information Security Culture	12
Systemic Security Management: A Total Systems Perspective	13
Evolving the Information Security Program.....	14
Spiral Model SM Implementation Strategy	14
Information Security Reference Documents.....	16
Laws, Regulations, and Legal Responsibilities	16
Information Security Governance.....	16
Best Effective Information Security Practices	17
Information Security Management Guides, Standards and Practices	17
Technology Configuration Guides.....	18
Information Crime Surveys.....	18
Key Web Sites.....	18
Citadel Information Group.....	18
Appendix: Pro-Forma Information Security Policy “Table of Contents”	20

Purpose of this White Paper

The management of sensitive information is in a state of crisis. Over the last two years, businesses and other organizations have sent out more than 100,000,000 letters to Americans everywhere that their supposedly-private personal financial information has been lost to cyber-criminals. Corporate intellectual property is every bit as much at risk ... including financial information, sensitive sales and pricing information, private information of employees, key corporate strategies, proprietary processes, etc. If information has value, it is at risk.

Never before has the confidentiality, availability and integrity of critical organizational information been so threatened. The threat is great and it is growing.

As a result of this increasing threat, the fact that every part of the organization is vulnerable, and the underlying reality that solving the information security challenge requires senior management attention and leadership, senior executives have begun to pay increasing attention to securely managing critical information assets.

The purpose of this *Citadel White Paper* is to provide guidance to senior executives who are charged with designing and implementing a cost-effective program to secure critical information assets.

The Information Security Management Program

Every organization has an *information security management program*. The *program* consists of the totality of all activities and expenditures the organization takes to protect sensitive information. The program may be formal with a specific executive tasked with management responsibility, or it may be informal with activities and expenditures spent as needed. Formal or ad hoc, proactive or reactive, effective or not, every organization manages the security of its critical information.

Thus the key question is not “Do you need an information security management program?”

The key question is “How effective is your information security program.”

Information Security Management Program Objectives

The objective of an organization's *Information Security Management Program* is to prudently and cost-effectively manage the *risk* to critical organizational information assets.

- The risk that critical information is compromised
- The risk that critical information becomes unavailable
- The risk that critical information is changed without authorization

Associated with *risk* is *cost*. Security incidents cost money. So does preventing them.

The cost, for example, of a computer virus is the loss in productivity of an organization's personnel plus the time and expense for IT personnel to remove the virus and restore availability. The cost of a theft of a trade secret by a cyber-thief is the value of the trade secret. The cost of the theft of customer social security numbers is the cost of notifying customers plus any identity theft expenses provided to protect customers plus any legal expenses if there are law suits plus the loss of good will.

Implementing security also has costs. Firewalls and other security technology takes capital away from other uses. Information security personnel come at the expense of personnel who can directly more contribute to the bottom line. And every hour management spends in a security meeting, or personnel spend on security awareness training, is an hour that could otherwise also contribute to the bottom line.

Thus the objective of any information security management program is to be like *Goldilocks*. Not too much. Not too little. Just right.

Recalling Philip Crosby's book *Quality is Free*¹ and his seminal definition of the *total cost of quality*, one can analogously assign costs to security incidents and security prevention:

<i>Incident Recovery Costs</i>	<i>Security Prevention Costs</i>
<ul style="list-style-type: none">• Direct recovery costs• Costs for lost productivity• Fraud & embezzlement losses• Intellectual property losses• Legal & attorney costs• Costs to value of brand• Indirect community costs	<ul style="list-style-type: none">• Firewalls, Anti-Virus & Other Technology• Security Management Costs, including executive management , IT management and security management• Security Overhead Costs, including productivity loss from training, direct overhead from security controls, etc.

With the above in mind, one can alternatively define the objective of an organization's *Information Security Management Program* as minimizing the "*Total Cost of Security*."

¹ *Quality is Free*, Philip Crosby, Mentor Books, 1980

Evolving Requirements for an Information Security Management Program

The drivers behind an organization's information security management program are the evolving landscape of laws, regulations, and competition, as well as evolving information security "best effective" practices.²

Organizations that hold personal, financial or health information of others are required to adhere to various federal and state laws and regulations. These include

- Gramm-Leach-Bliley (personal financial information)
- HIPAA (electronic protected health information)
- Sarbanes-Oxley, Paragraph 404
- FTC Safeguards Rule
- FTC Regulation of Unfair and Deceptive Practices
- CA Civil Code 1798.84 Breach Disclosure (non-public personal information)
- CA 1798.81.5 (reasonable security measures)

Organizations may also have various contractual requirements for information or data security. Credit card processors, for example, must conform to the *Payment Card Industry Data Security Standard*.³

As organizations come to more deeply understand the competitive value of the information stored in their computer networks and the need to make that information securely available anytime and anywhere, they discern the need for a formal information security management program to assure that information is kept confidential, available, and correct..

An Arkansas court recently held that a company was not entitled to intellectual property protection because its information security controls were not adequately strong. Thus, the need to protect one's trade secrets is also acting to push an organization into proactive management of its information assets.⁴

As organizations have increasing needs to share information with suppliers, customers, and other business relations they are increasingly becoming concerned with the information security capabilities of these third parties.

² For an overview of these, see *An Emerging Information Security Minimum Standard of Due Care*, Robert Braun, Esq., Stan Stahl, Ph.D, Information Security Management Handbook, Fifth Edition, Vol 2, Auerbach, 2005 and *An Emerging Information Security Minimum Standard of Due Care*, Robert Braun, Esq., Stan Stahl, Ph.D, Privacy & Data Security Law Journal, March 2006.

³ *Payment Card Industry Data Security Standard, Version 1.1*

⁴ *Open Secrets: Can You Claim Your Trade Secrets Were Stolen If Your Security Was Sloppy*, CSO Online, June 2004

Needs for third-party assurance are also driving an industry of information security auditors. Increasing numbers of organizations are having their information security audited by third-parties. These information security audits are often a condition of information sharing. These kinds of information security audits may also be undertaken as a means of achieving a particular security designation. Examples include the *SAS-70 Type II* certification, which is quickly becoming a necessity for data centers, and the *PCI Certification* for credit card merchants and processors.

An organization’s information security management program must be built upon current and emerging information security “effective best-practices.” As the information security industry has evolved, the industry has tended to settle on three distinct models as to what constitutes a set of “effective best-practices” for managing the security of information: ^{5,6}

- ISO-27001 Specification for an Information Security Management System
- ISO-17799: Code of Practice for Information Security Management
- CISSP: Certified Information Systems Security Professional
- ISACA: Information Security “Management Maturity Model”

Managing the Security of Critical Information Assets

Information Security Control Objectives

While the prevailing ‘consumer perspective’ of information security is that it is concerned with protecting the confidentiality of sensitive information, information security actually has 16 control objectives.

	Protect	Detect	Recover	Comply
<i>Confidentiality</i>	✓	✓	✓	✓
<i>Integrity</i>	✓	✓	✓	✓
<i>Availability</i>	✓	✓	✓	✓
<i>Authentication</i>	✓	✓	✓	✓

⁵ See also *GAISP: Generally Accepted Information Security Practices*, under development by the ISSA.

⁶ These “effective best-practices” are described in some detail in *An Emerging Information Security Minimum Standard of Due Care*, Robert Braun, Esq., Stan Stahl, Ph.D, *Information Security Management Handbook*, Fifth Edition, Vol 2, Auerbach, 2005.

These control objectives recognize that it is not enough to put all of one's security resources on protecting information. Information is under stealth attack and it is only prudent to commit resources to detecting attacks and to be sure that one can recover from attacks. And while compliance is linked to the other three "columns" it requires management oversight and corporate resources as well.

Defense-in-Depth with Feedback

Defense-in-depth means that no single vulnerability will result in the compromise of critical information; if a cyber criminal gets through one barrier, he'll soon run into another. A compromised user password might allow a cyber-criminal onto the corporate network but with *defense-in-depth* he still won't be able to access a server containing social security numbers. For that, he'll need to exploit another vulnerability. And even if he gets on the server, *defense-in-depth* will keep him out of the social security database.

Feedback means that management is "watching" the network and so is better able to protect information assets. With *feedback*, management would have a log entry showing the cyber-criminal accessing the network and it would be alerted when the cyber-criminal started to attack the server. If the cyber-criminal found a way onto the network without a password, a robust *feedback* system could notify management at that point.

The Fundamental Equation of Information Security⁷

The following equation illustrates the inter-relationships of the four primary information security variables.

$$\text{Information Risk} = \frac{\text{Threats} * \text{Vulnerabilities}}{\text{Countermeasures}}$$

As discussed above, the management objective of the *information security management* program is to prudently and cost-effectively manage *Information Risk*.

Threats to information are, for example, cyber thieves, competitors, disgruntled employees, foreign agents, earthquakes, etc.

Vulnerabilities are weaknesses that allow a threat to attack information. Examples include unpatched servers and workstations, inadequately managed access control, weak passwords, untrained personnel, ill-defined employee termination procedures, inadequate incident response, disaster recovery and information continuity planning, etc.

⁷ The *Fundamental Equation of Information Security* was developed at TRW in the mid-1980s by Frank Quigley and Stan Stahl. The equation was developed in response to the need by the Defense community for a risk characterization aligned with the need to protect information confidentiality and ensure information availability. This is analogous to the predominant information security needs of 21st-century organizations.

Countermeasures are those management actions taken to lower *Information Risk* to acceptable levels. These include improved technology and technology management, formal policies, employee training, and formal management structures.

As the equation illustrates, *information security vulnerabilities* increase information risk while *information security countermeasures* decrease risk. Successfully managing information risk, therefore, lies in knowing one's *vulnerabilities* and applying effective *countermeasures* to them.

Countermeasure Control Classes

The information security industry has recognized three broad countermeasure control classes:⁸

- Administrative
- Technical
- Physical

Administrative controls include policies, standards, procedures, guidelines, personnel screening, awareness training, etc.

Technical controls include network logins and passwords, firewalls, audit logs encryption, anti-virus and Spam filters

Physical controls include door locks, cameras, environmental controls, guards, etc.

BeBop Masters' intends to implement our *defense-in-depth with feedback* strategy with a combination of administrative, technical and physical controls.

Information Security Critical Success Factors

Information security has seven *Critical Success Factors* which must be implemented if an organization is to meet its information security control objectives.⁹

1. **Executive Management Responsibility:** Senior management has responsibility for the firm's information security program, and this program is managed in accordance with the enterprise's information security policies.
2. **Information Security Policies:** The enterprise has documented its management approach to security in a way that complies with its responsibilities and duties to protect information.
3. **User Awareness Training & Education:** Information users receive regular training and education in the enterprise's information security policies and their personal responsibilities for protecting information.

⁸ See, for example, *All-in-One CISSP Certification Exam Guide*, Shon Harris, McGraw-Hill,

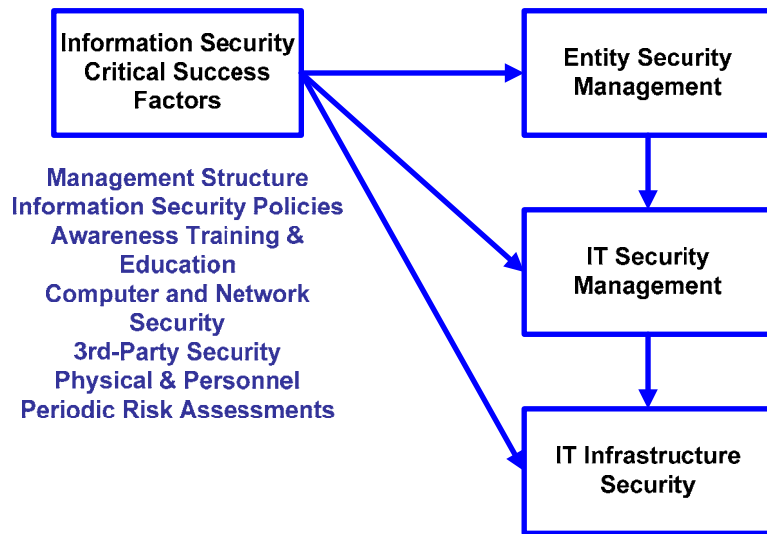
⁹ These are identified in *An Emerging Information Security Minimum Standard of Due Care*, Robert Braun, Esq., Stan Stahl, Ph.D, *Information Security Management Handbook*, Fifth Edition, Vol 2, Auerbach, 2005.

4. **Computer and Network Security:** IT staff and IT vendors are securely managing the technology infrastructure in a defined and documented manner that adheres to effective industry information security practices.
5. **Physical and Personnel Security:** The enterprise has appropriate physical access controls, guards, and surveillance systems to protect the work environment, server rooms, phone closets, and other areas containing sensitive information assets. Background investigations and other personnel management controls are in place.
6. **Third-Party Information Security Assurance:** The enterprise shares sensitive information with third parties only when it is assured that the 3rd-party appropriately protects that information.
7. **Periodic Independent Assessment:** The enterprise has an independent assessment or review of its information security program, covering both technology and management, at least annually.

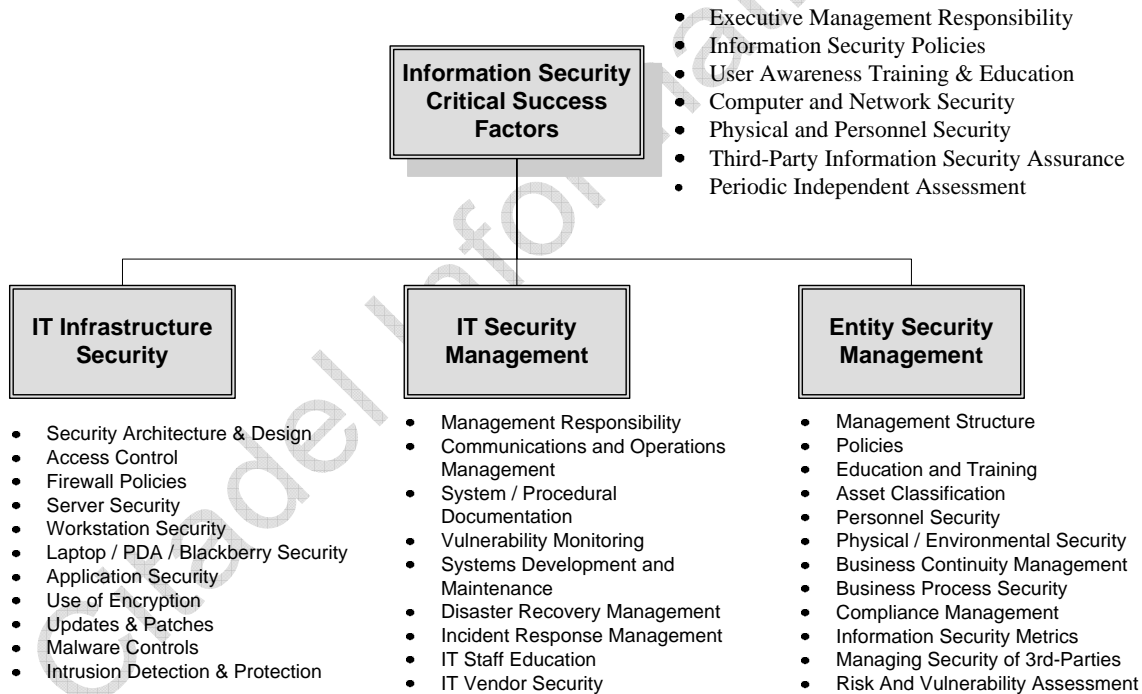
Management Control Domains

These seven critical success factors play themselves out across three fundamental management control domains:

1. **IT Infrastructure Security:** Control elements in this domain identify specific point-in-time technical information security countermeasures. Examples include the security architecture; firewall rules; technical access controls; backup status; use of encryption; virus, worm, Trojan horse prevention; current patch levels; intrusion detection capabilities; etc.
2. **Secure IT Management:** This control domain contains information security management controls specific to managing the Information Technology infrastructure. Control elements in this domain include documentation of IT systems, procedures, etc; management of systems development and maintenance processes, including change control; incident response and disaster recovery planning; IT staff education; IT vendor security; etc.
3. **Entity Security Management:** This control domain contains management controls hierarchically “above” and outside of the management of the Information Technology infrastructure. Control elements in this domain include the chief information security officer, information security policies, employee education and awareness training, business process security, physical security, personnel security, etc.



The following chart takes these 3 management control domains to the next level of detail:



Managing the Information Security Program

Chief Information Security Officer (CISO)



Responsibility and authority for information security matters resides with a *Chief Information Security Officer (CISO)*. The *Chief Information Security Officer (CISO)* often reports to a COO, CFO or CIO. As organizations come to recognize the criticality of information to their ongoing survival, more and more often the *CISO* is getting his or her own seat at the executive table.

Information Security Steering Committee

The *CISO* is supported by a cross-functional *Information Security Steering Committee*. In order to make sure that information security leadership and management extends across the organization, *Steering Committee* members need to include senior representatives of marketing, sales, operations, HR, finance and IT. Formal appointment to the *Information Security Steering Committee* is made by the *COO* in consultation with the *CISO*.

Citadel Information Group

Information Security Responsibilities

Everyone in an organization has a role to play in securing the organizations critical information assets. The following table provides an overview of these responsibilities.

<i>Functional Role</i>	<i>Security Responsibilities</i>
Chief Executive Officer	<ul style="list-style-type: none">• Oversees and is accountable for overall security capacity
Chief Information Security Officer & Steering Committee	<ul style="list-style-type: none">• Provide leadership• Establish policies• Coordinate implementation• Responsible for risk and vulnerability assessment
Managers & Staff	<ul style="list-style-type: none">• Implement policies & procedures• Be aware• Be vigilant• Report vulnerabilities & attempted breaches
IT Organization	<ul style="list-style-type: none">• Secure the IT infrastructure• Securely manage IT• Respond to incidents, breaches & disasters• Increase knowledge, skills and capabilities

Creating an Information Security Culture ¹⁰

The effectiveness of an information security program ultimately depends upon the behavior of people. Behavior, in turn, depends upon what people know, how they feel, and what their instincts tell them to do. While information security policies, an awareness training program and the other required information security practices can define, regulate and impart information security knowledge these rarely have significant impact on people's feelings about their responsibility for securing information, or their deeper security instincts. The result is often a gap between the dictates of information security policy and the behaviors of our people.

Until and unless we affect how people feel about the need to secure information ... until and unless our people develop good information security instincts ... the gap between the dictates of information security policy and the behaviors of people will persist.

It is the role of culture to close this gap. ¹¹

¹⁰ See *Beyond Information Security Awareness Training: It's Time to Change the Culture*, Stan Stahl, Ph.D., *Information Security Management Handbook, Fifth Edition, Volume 3*, edited by Hal Tipton and Micki Krause, Auerbach, 2006.

Systemic Security Management: A Total Systems Perspective ¹²

A new conceptual framework for information security has recently been developed at USC's *Institute for Critical Information Infrastructure Protection* in collaboration with the *American Center for Strategic Transformation*. The framework provides a robust model for information security cultural change. It does this, in part, by extending the more traditional 3-node *people, process, technology* linear framework through which information security is traditionally considered to a dynamic non-linear framework that includes *organizational design* and *strategy*.

The addition of the *organizational design* and *strategy* node to the classical 3-node framework introduces a powerful leverage point for proactive information security culture change. The framework also introduces three *dynamic tensions* linking *organizational design* and *strategy* to *people, process, and technology*: *culture, governance, and architecture*.

Taken in its totality, this new framework identifies 10 *leverage points* for information security evolution: four nodes and six tensions.

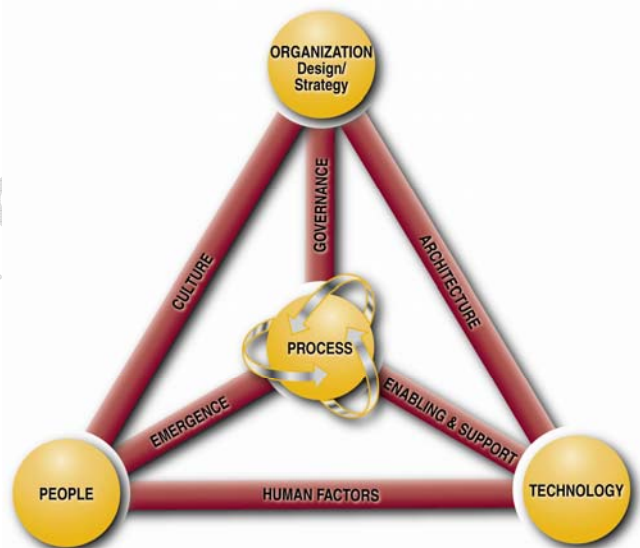
Nodes:

- Organizational Design / Strategy
- People
- Technology
- Processes

Tensions:

- Human Factors
- Culture
- Governance
- Architecture
- Enabling & Support
- Emergence

It is through the creative management of these ten leverage points that the management can evolve its desired proactive information security capability.



¹¹ *Organizational Culture and Leadership*, 2nd Edition, Edgar H. Schein, Jossey-Bass, 1992, defines the culture of an organization as *a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.*

¹² *Systemic Security Management: A New Conceptual Framework*, Laree Kiely, Ph.D. & Terry Benzel, 2006.

Evolving the Information Security Program

Spiral ModelSM Implementation Strategy

While auditors, Boards, and the CEO may want senior management to ‘snap its fingers’ and *voila, security is arrived*, the real world insists otherwise. As the industry has learned, information security is an ongoing process of balancing evolving threats and vulnerabilities with cost-effective countermeasures so as to keep residual risk at acceptable levels. In this way, information security program management is like other performance improvement challenges and is, therefore, amenable to the same strategies as have proven effective in other performance improvement domains.

Every formal performance improvement programs is based on a *performance improvement methodology*, along the lines of, for example Deming’s famous *Plan-Do-Check-Act* methodology for improving manufacturing systems.

A similar model, better suited to the continuous improvement of systems of management than is Deming’s, is *Citadel’s* proprietary *Spiral ModelSM*.¹³ The *Spiral Model* is a powerful easy-to-use methodology for evolving performance systems, including information security management systems.

The *Spiral Model* supports continual learning and the application of that learning to the information security needs of the organization. And it does so in real-time, at the moment of need, supporting what Fritz Dressler has called “evolution on the fly.”

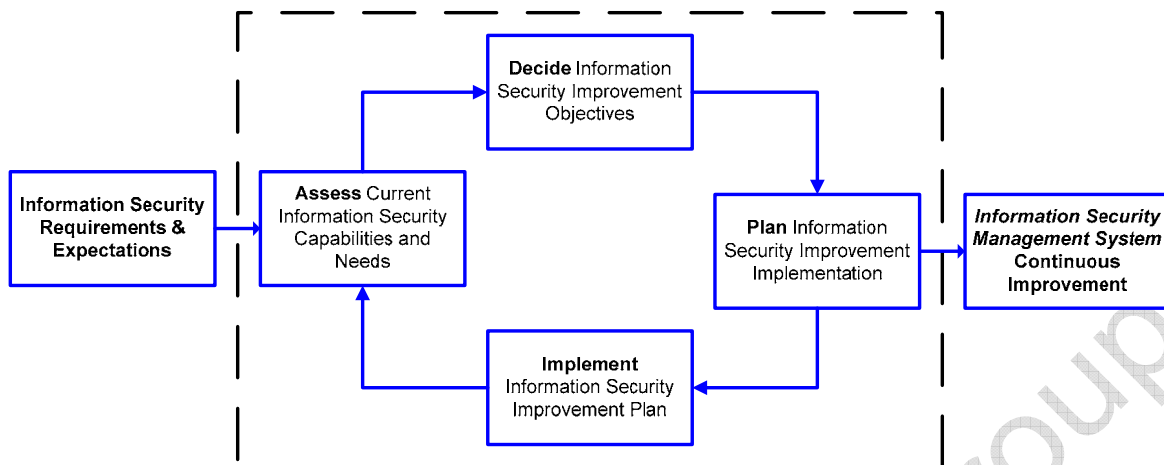
The *Spiral Model* has its origins in three earlier performance methodologies. One is the famous *Plan-Do-Check-Act* method taught by Deming. A second is the OODA cycle—*observe, orient, do, act*—that emerged in fighter pilot studies in the 1950s. The third is a systems development methodology developed at TRW. Like the *Spiral Model*, all embrace the fundamental arrow of purposeful evolution: Action, Feedback, Synthesis.

There are four basic steps to the *Spiral Model*:

- *Assess* the situation
- *Decide* what to do to improve the situation
- *Plan* the improvement project
- *Implement* the improvement plan

The *Spiral Model* is illustrated in the following diagram.

¹³ *Spiral Model* is a proprietary methodology of Citadel Information Group, Inc.



Critical to the use of the *Spiral Model* is to properly scope each cycle's *assessment*. An absolutely complete information security risk and vulnerability assessment would look at every component of a company's security program down to a level akin to counting paper clips. It would be a top-to-bottom assessment of the complete organizational security profile and it would look deeper than any cyber criminal might, far beyond the value of the information in need of protection. Obviously, this level of assessment would be a waste of time and a waste of money.

In order to properly scope the information security risk and vulnerability assessment it is important to consider the assessment in the broader context of an organization's ongoing need to improve its information security risk profile.

Using this chart, one scopes an information security risk and vulnerability assessment as follows:

- Identify information security requirements and expectations.
- Map these requirements and expectations against the seven critical success factors and three management control domains. This provides the total "context" for the organization's information security management program. It also establishes the total extent of the information security risk and vulnerability assessment.
- Considering organizational budget, information security requirements, and the current knowledge of your security profile, identify the specific components to be assessed during the current *Spiral*. This can be a complete assessment, a component assessment, or even a sub-component (assess compliance with customer requirements, assess the business continuity plan, etc). Also identify the depth to which these components are to be assessed.¹⁴
 - There are two complementary strategies for scoping a formal assessment
 - *Top-Down Strategy*: The available budget is spread somewhat equally across all assessment components. The depth of the assessment is then determined by the available budget

¹⁴ This step is based on the principle that one eats an elephant one bite at a time.

- *Bottom-Up Strategy*: In this strategy a particular component is assessed as deeply as available budget allows

What makes both of these strategies work is the knowledge that an assessment is just one step of an ongoing management process to effectively secure the organization's critical information assets. As the *Spiral Model* illustrates, one will have ongoing opportunities to increase the breadth and the depth of subsequent information security assessments.

Information Security Reference Documents

Laws, Regulations, and Legal Responsibilities

Federal Laws & Regulations

1. Office of Comptroller, Privacy of Consumer Financial Information, 12CFR 40
2. Federal Trade Commission, Standards for Safeguarding Customer Information, 16CFR14
3. HIPAA, 45 CFR Parts 160 and 164
4. 2002, August 14, 2002, February 2003, and April 17, 2003
5. Sarbanes-Oxley, Paragraph 404

California Civil Code

6. Breach Disclosure Law (CA-1386), CA Civil Code 1798.80-84
7. Reasonable Security Procedures and Practices, CA Civil Code 1798.81.5
8. California Business Privacy Handbook,
http://www.privacy.ca.gov/business/ca_business_privacy_hb.pdf

Other Legal

9. An Emerging Information Security Minimum Standard of Due Care, Robert Braun, Esq., Stan Stahl, Ph.D, Handbook of Information Security, Auerbach, 2004
10. An Emerging Information Security Minimum Standard of Due Care, Robert Braun, Esq., Stan Stahl, Ph.D, Privacy and Data Security Law Journal, March 2006
11. Open Secrets: Can You Claim Your Trade Secrets Were Stolen If Your Security Was Sloppy, CSO Online, June 2004

Information Security Governance

12. Information Security Governance: Guidance for Boards of Directors and Executive Management, Information Systems Audit & Control Foundation, ISACA, 2001
13. Securing Cyberspace - Business Roundtable's Framework for the Future, 2004

14. Information Security Governance, National Cybersecurity Partnership, 2004

Best Effective Information Security Practices

15. Specification for an Information Security Management System, ISO-27001: 2005
16. Information Technology—Code of Practice for Information Security Management, International Standards Organization, ISO-17799, 2000
17. Information Security Management Systems—Specification with Guidance for Use, BS-7799-2:2002
18. Generally-Accepted Information Security Principles (GAISP), Version 3.0 (Draft), The Information Systems Security Association, 2004
19. Payment Card Industry Data Security Standard, Version 1.1

Information Security Management Guides, Standards and Practices

20. National Institute of Standards & Technology, Information Security Handbook: A Guide for Managers (Draft), SP800-100
21. National Institute of Standards & Technology, Guide to Intrusion Detection and Prevention (IDP) Systems, SP800-94
22. National Institute of Standards & Technology, Guide to Computer Security Log Management, SP800-92
23. National Institute of Standards & Technology, Guide to Integrating Forensic Techniques into Incident Response SP800-86
24. National Institute of Standards & Technology, Guide to Malware Incident Prevention and Handling, SP800-83
25. National Institute of Standards & Technology, Security Considerations in the Information System Development Life Cycle, SP800-64
26. National Institute of Standards & Technology, Computer Security Incident Handling Guide, SP800-61
27. National Institute of Standards & Technology, Security Considerations for Voice Over IP, SP800-58
28. National Institute of Standards & Technology, Building an Information Technology Security Awareness and Training Program, SP800-50
29. National Institute of Standards & Technology, Security Guide for Interconnecting Information Technology Systems, SP800-47
30. Others available, as well; *see NIST web site*

Technology Configuration Guides

31. Windows Server 2003 Security Guide, NSA, April 26, 2006
32. Others available, as well; *see NSA web site*

Information Crime Surveys

33. 2006 CSI/FBI Computer Crime and Security Survey

Key Web Sites

34. CERT Coordination Center / Carnegie Mellon University: <http://www.cert.org/>
35. National Institute of Standards and Technology (NIST) Computer Security Resource Center: <http://csrc.nist.gov/>
36. SANS Institute: <http://www.sans.org/about/sans.php>
37. National Security Agency (NSA) Information Assurance Program: <http://www.nsa.gov/ia/index.cfm>
38. Information Systems Security Association – LA Chapter: <http://www.issa-la.org/default.aspx>
39. Citadel Information Group: www.citadel-information.com

Citadel Information Group

Citadel Information Group is an *Information Security Management Services* firm headquartered in Los Angeles, CA. Our objective is to provide clients with a full-range of information security management services, whether to act as their information security department or to augment their existing information security infrastructure. The firm was founded in 2002 by Dr. Stan Stahl and Ms. Kimberly Pease, CISSP.

Dr. Stahl's information security career began in 1980 when he assisted NORAD secure a database management system to distinguish space objects from enemy nuclear missiles. Over the course of his career Dr. Stahl has provided information security support to the *White House*, *Strategic Air Command*, *NASA* and other government agencies. Dr Stahl serves as *President* of the Los Angeles Chapter of the *Information Systems Security Association*.

Ms. Pease is a former *Chief Information Officer* for a mid-sized printing company. Her CIO responsibilities included managing day-to-day tactical IT operations and for aligning IT with the strategic focus of the company. Her achievements include leading the company's ISO 9002 and ISO 14001 initiatives, achieving corporate-wide technology standardization, and ensuring Y2K compliance. Ms. Pease has achieved designation as a *Certified Information Systems Security Professional*. She serves as *Education Director* of the Los Angeles Chapter of the *Information Systems Security Association*.

Citadel Information Group designs and implements information security management programs to meet client needs for effective information security risk management. The scope of our services extends from the firewall to the Board Room.

Citadel's services include information security risk and vulnerability assessments, penetration testing, policy development, business continuity & disaster recovery (BCP/DR), incident response, IT management support, 3rd-party security management, technology hardening, eDiscovery & forensics, awareness training security governance, and creating an information security aware culture.

Our clients come from a wide range of industries, including financial services; healthcare; law, accounting & other professional services; manufacturing, distribution & logistics; eBusiness, media, retail, government and education. We are proud to count several not-for-profits among our clients, believing in the importance of serving this traditionally under-served community.

The firm has built a strong reputation in the community based on the high quality of our services and our excellent customer service.

Here's what some of our satisfied clients have to say about us:

Thanks for helping us pass our challenging and extensive Payment Card Industry information security audit. Your information security management services perfectly augmented our own. This let us get through the audit efficiently and cost-effectively. Mark Goldin, Chief Information Officer & EVP Operations, Green Dot Corporation.

Having used you as RBZ's information security team, I know that when we refer a client to you, you'll make us look good. You have an amazing ability to discover information security weaknesses where others aren't even looking. Tom Schulte, Managing Partner, RBZ, LLP.

Citadel Information Group represents high integrity, an exceptional skill set, and a dedication to my organization. Citadel has repeatedly stepped up to meet the challenges we have presented them with, and even when difficult, they have risen to the occasion. David Lam, Director of IT, Stephen S. Wise Temple.

Citadel has helped ECF strengthen our IT network and secure our clients' confidential information. The result is not just better security but also a greater ability to effectively meet our mission to serve people with developmental disabilities, less money spent on IT, and a better night's sleep for me. Scott Bowling, Psy D., President & CEO, Exceptional Children's Foundation

Thanks so much for everything. I TRULY enjoyed working with all of you. You threw me a lifesaver and pulled me in when I was surrounded by sharks. I'll never forget that. Donna Nakawaki, CFO, Rem Eyewear

Appendix: Pro-Forma Information Security Policy

“Table of Contents”

1.	Introduction	
1.1.	Commitment to Securing Information Assets.....	5
1.2.	Information Security Policy Objectives.....	5
1.3.	Scope of These Policies	5
1.4.	Compliance is Essential	6
1.5.	Waiver of Policies.....	6
1.6.	Miscellaneous Policies.....	6
1.7.	Further Information.....	7
2.	Information Security Management	8
2.1.	Summary	8
2.2.	Chief Information Security Officer.....	8
2.3.	Information Security Steering Committee	8
2.4.	Information Security Decision Making Authority	9
2.5.	3 rd -Party Security Management	9
2.6.	Business Continuity Management	9
3.	Information Classification & Control	11
3.1.	Summary	11
3.2.	Information Assets	11
3.3.	Information Owners, Users, and Custodians	11
3.4.	Security Classification of Information.....	12
3.5.	Access to Restricted Information Requires Business-Related Need-to-Know.....	13
3.6.	Restricted Media Management	13
3.7.	Security Classification of Information Assets	13
4.	Physical Security.....	15
4.1.	Summary	15
4.2.	Physical Locations	15
4.3.	Perimeter Security.....	15
4.4.	Physically Securing Server Rooms.....	15
4.5.	Visitor Control	16
4.6.	Janitor Control	16
5.	Personnel Security	17
5.1.	Summary	17
5.2.	Security in Job Definition and Staffing	17
5.3.	Background Investigations.....	17
5.4.	Confidentiality Agreement.....	17
5.5.	Employee Termination and Absence Notification.....	17
6.	Policies for Employees and Other Information Users	18
6.1.	Summary	18
6.2.	Ownership & Control of Information Systems.....	18
6.3.	Access Control	18
6.4.	Workstation Security	20
6.5.	Electronic Mail.....	20
6.6.	Information Security Investigations.....	21

6.7.	Technology Prohibitions.....	22
6.8.	Protecting Information Using Encryption.....	23
6.9.	Physical Protection of Confidential Information	23
6.10.	Information Security Training and Education	24
6.11.	Other User Responsibilities	24
7.	IT Infrastructure Policies	26
7.1.	Summary	26
7.2.	Director of IT	26
7.3.	Secure Network Design and Build.....	26
7.4.	Secure Network Maintenance	29
7.5.	Change Control	30
7.6.	Access Control Management	31
7.7.	Need-to-Know Control Based Upon Job Requirement	33
7.8.	Device Usage Control	33
7.9.	Remote Access Management.....	34
7.10.	Restricted Information at Rest	35
7.11.	Restricted Information in Transit.....	35
7.12.	Encryption Key Management	36
7.13.	Logging and Review	36
7.14.	Backup & Recovery	38
7.15.	Incident Response & Investigations.....	38
7.16.	Information Continuity	39
7.17.	Other IT Infrastructure Policies	40
7.18.	Information Security Training and Education	41
8.	System and Application Development Policies.....	42
8.1.	Summary	42
8.2.	VP Technology	42
8.3.	Separation of Development and Production Systems.....	42
8.4.	Development Life-Cycle.....	42
8.5.	Development Requirements for Restricted Systems.....	43
8.6.	Development Training and Education	44