CITADEL
INFORMATION GROUP, INC.

A Success Strategy for Information Security Planning and Implementation

A guide for executives

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

www.citadel-information.com
2060 Hercules Drive
Los Angeles, CA 90046
Tel: 323.876.1441
Fax: 323.876.7794

TABLE OF CONTENTS

THE INFORMATION SECURITY PLANNING CHALLENGE

Like any kind of project, an information security project requires the successful management of ten key elements:

1. Project scope
2. Project time & schedule
3. Project cost & budget
4. Project resources, internal and external
5. Contract management
6. Procurement management
7. Project communications
8. Quality management
9. Project risk
10. Cross-organizational coordination

In addition to the above, information security projects have their own particular management challenges inhibiting project success:

- Information security projects usually lie outside the core functions of the business, increasing the likelihood that other business needs will divert critical management attention and resources.
- Except in some pure technology implementation projects, information security projects often require the coordination and buy-off of different constituencies, increasing the likelihood that differing business constraints and perspectives will make decision-making more difficult.
- Also making decision-making more difficult is that, except again in some pure technology implementation projects, information security projects often involve making trade-offs between increasing security and maintaining productivity.

PREPARING TO MEET THE CHALLENGE: THE SPIRAL MODEL SM

The first step is in meeting information security planning challenges is to recognize that a particular information security project (or set of projects) is simply a part of a company's ongoing information security program.

Threats, risks, vulnerabilities, and the counter-measures for dealing with them are constantly changing. No matter how secure you are today, if a new exploit is discovered, your defenses may be for naught.

Information security is a never-ending process of ongoing improvement. The objective is not 100% security. One hundred percent total security is not achievable, and even if it could be it would be prohibitively expensive and way out of line with the value of the information being protected. Information security is not about certainty; it is about continually balancing evolving threats and vulnerabilities with cost-effective countermeasures so as to keep residual risk at acceptable levels.

The fact that information security is an ongoing process means that an information security project is simply an ongoing element of a succession of information security projects, an overall *Information Security Program*, so to speak.

Because each information security project is part of an overall *Information Security Program*, Citadel has developed a proprietary *Spiral Model* [SM] that we use to successfully manage an organization's information security program in a strategically sound way. [1]

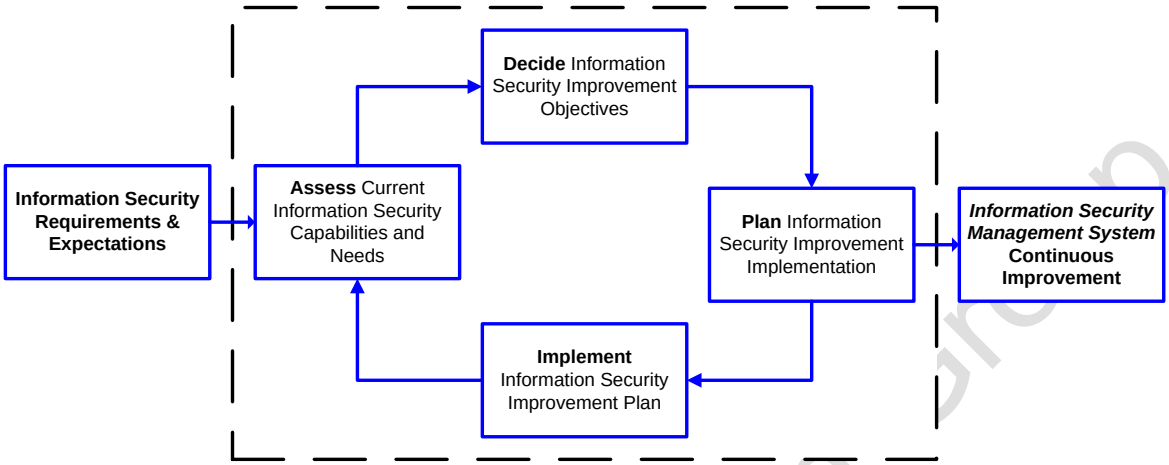
The *Spiral Model* has its origins in three earlier process improvement methodologies. One is the famous *Plan-Do-Check-Act* method taught by the famous quality management consultant W. Edwards Deming. A second is the OODA cycle—*observe, orient, do, act*—that emerged in fighter pilot studies in the 1950s. The third is a *spiral* 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

[1] *Spiral Model* is a proprietary methodology of Citadel Information Group, Inc.

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



GETTING STARTED: THE INFORMATION SECURITY ASSESSMENT

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.[2]

  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
  - *Bottom-Up Strategy:* In this strategy a particular component as 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.

BEFORE YOU PLAN: THE DECISION WORKSHOP

Sometimes the results of an assessment are straightforward and it is obvious what needs to be done and in what order.

More often though, particularly early on in an organization's formal information security management program, an assessment will surface numerous things that prudence suggests should be done, with the challenge that it is not at all obvious what improvements should be done and in what order.

It is in these situations that the greatest danger of sub-optimization occurs. The more complicated the range of options and the greater the business constraints, the more important it is to carefully decide how corporate resources are going to be used to address information security challenges.

The quickest most cost-effective solution: a ***Decision Workshop***

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

Decision Workshops

A workshop (or sequence of workshops) is often the most effective way to quickly decide how corporate resources are going to be used to address information security challenges.

Workshops need to be carefully planned if they are to get quick results and minimize planning costs.

- Workshop goals and objectives need to be established and agreed upon.
- Workshop attendees need to be identified. All information security constituents – executive management, finance, IT, and personnel – should be considered for the workshop(s).
- Workshop agendas need to be carefully prepared and followed. Together with workshop goals and objectives, these should be provided to attendees prior to the workshop as should any preliminary reading.
- Workshops need to be action-oriented. While a lot of discussion is often necessary to sort out all the differing options and constraints, a workshop must lead to action.
- Workshops need to be documented, particularly critical discussion points and action items. These should be distributed to attendees for review and follow-up within 24 hours.
- Workshops also need to be consensus-based. Information security is challenging enough when everyone in an organization is on the same page. It's even more challenging when they're not.

PLANNING

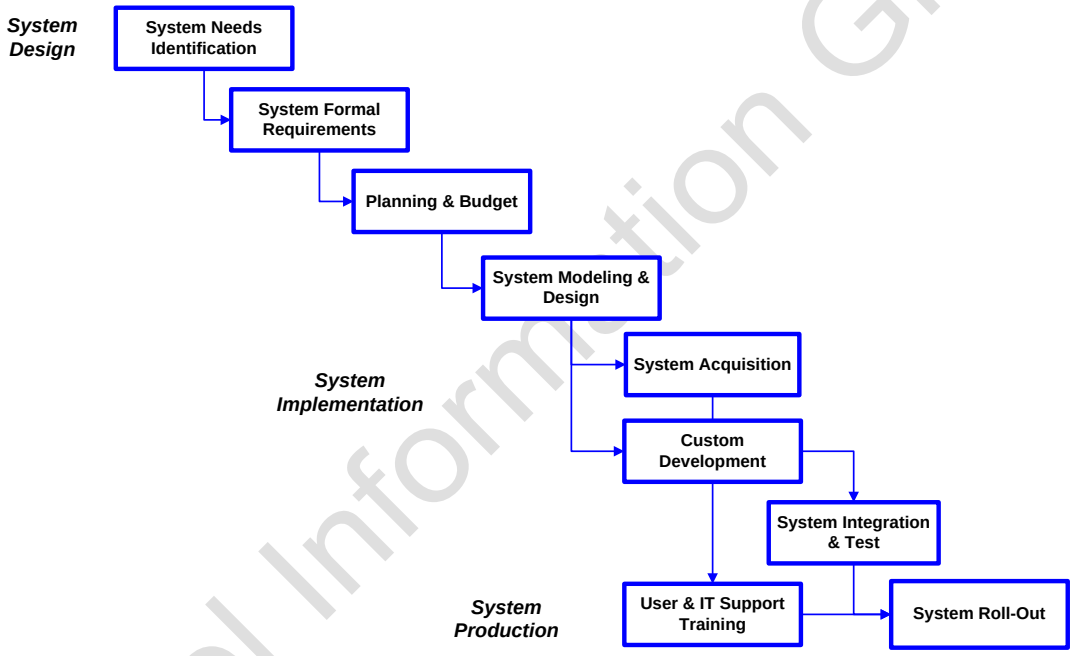
Once the *Decision* phase is completed, project planning can begin. In the best of worlds, planning can be done on the back of an envelope, with little risk to either the organization's security or its business. In other more complex cases, detailed plans will have to be developed to manage project risk.

Whether it's the back of an envelope (we recommend at least a rather large envelope) or a full blown plan, risk can be minimized by explicitly planning all ten project management elements:

1. Project scope
2. Project time & schedule
3. Project cost & budget
4. Project resources, internal and external

5. Contract management
6. Procurement management
7. Project communications
8. Quality management
9. Project risk
10. Cross-organizational coordination

A complex information security project may be complex enough to require a formal project implementation life-cycle, similar to the following.



The value in using a life-cycle is that it makes it easier to make sure work gets done in the right order: buying a firewall before documenting firewall requirements is just one way money and other resources can be wasted if steps occur out of order.

MANAGING IMPLEMENTATION

Successful information security implementations are the result of doing the following seven things right:

1. **Vigorously manage scope creep:** the biggest cause of project failure

2. **Conduct regular project review meetings:** Track progress against expectations, review challenges, and identify next steps
3. **Manage project metrics:** cost, schedule, resulting security, e.g., percent of fixed bugs, hosts with intrusion prevention, internet facing devices, percent of systems monitored, percent of staff trained, percent of 3rd-parties with security agreements, etc
4. **Manage to the life-cycle:** don't design before you know requirements
5. **Watch your risks:** commitments from outsiders, other needs for scarce resources, anywhere *Murphy's law* might be lurking; track top-10 at project review meetings; be prepared with contingencies
6. **Don't let things slip through cracks:** the devil is in the details
7. **Plan to change plans:** things rarely go as planned

When the implementation project is finished, it's time to assess again. This time, though, you can also assess how well you did as you went around the four steps of the *Spiral Model*:

- How valuable was the information you got from the assessment?
- Was your decision making effective?
- Did you underplan? Overplan?
- Did the implementation go as expected?

Armed with this information, you can develop *lessons learned* enabling you to be even more effective on you next go around the *Spiral*. This gives you *double-loop improvement*:

- **Loop 1:** You improve security by going around the *Spiral*
- **Loop 2:** You improve security by going around the *Spiral* more effectively

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 *Treasurer* 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, Chief Information Officer, 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