




Information Security in the Enterprise

A New Paradigm



Most Enterprises have become well versed at reacting to security events, effectively mitigating the probability of recurrence. What is needed today is business-driven pro-active Information Security.

Overview

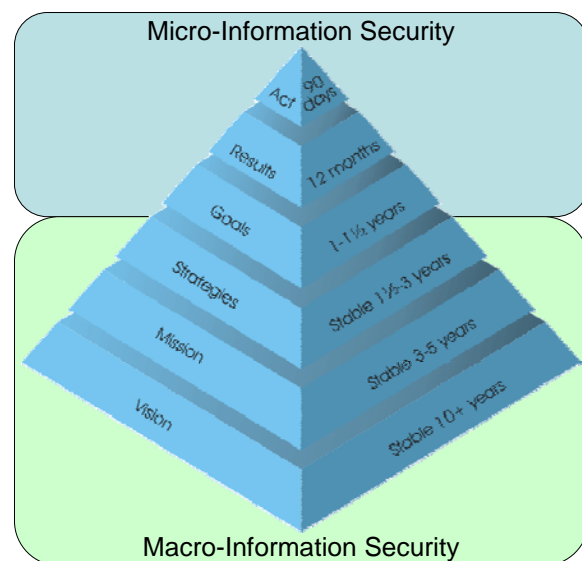
Information Security inside the corporation has evolved in last decade from a siloed, reactive endeavor to an accepted enterprise business practice. With this evolution it becomes obvious that information security and its constructs and underlying technologies must be fully integrated into the business. However, the continuing overuse of fear, uncertainty, and doubt (FUD), compliance edicts, audit findings, vulnerabilities, and credible threats have undermined the positive value proposition of information security to the lines of business. In turn, senior managers primarily responsible for information security find their positions in jeopardy when they are perceived as the impediment to growth and change, rather than a respected and contributing business management peer. This leads many business individuals outside of Information Technology to ask “What is *Information Security*” or possibly more accurately “What value does *Information Security* provide me”, thus complicating business integration and convergence.

The challenge becomes how to best ensure this integration. More than trial and error and experience are required. All information security professionals – engineering, operations, administration, compliance, and ISO (Information Security Officers) personnel – need to become knowledgeable in a new vernacular, *information protection stewardship*. They should be comfortable in verbalizing the tenants to not only their management, but also to the equivalent layer within the lines of business. They should have familiarity and be able to readily access knowledge of economics and business theory to aid them in socializing security initiatives.

As an example of the application of this let’s look at two terms from economics - *Microeconomics* and *Macroeconomics*. Microeconomics deals with economic behaviors at the individuals’ level, what is being bought and sold, and what is driving the decisions to allocate limited resources. Macroeconomics, on the other hand, involves the “sum total of economic activity, dealing with the issues of growth, inflation and unemployment, and with national economic policies relating to these issues.”

The concepts of Micro and Macro can be readily applied to an information security model. Micro-information security is defined as the technology, controls, countermeasures, and tactical solutions employed day-to-day to defend against cyber threats. It’s the nuts and bolts that support the corporation’s information security practice. It can be reduced to a step-by-step guide for securing the enterprise given the current set of requirements. By nature, it is fully reactive.

Macro-information security is defined as business structures and plans that influence and protect our enterprise. It is the “big picture” which can be leveraged to keep management in the loop. It’s the blueprint, framework, strategic plan, road map, governance, and policies designed to influence and protect the enterprise. It’s the *bottom line*.

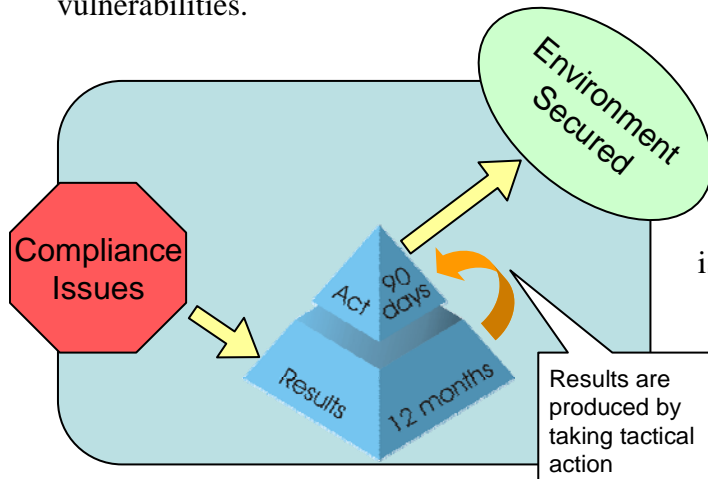
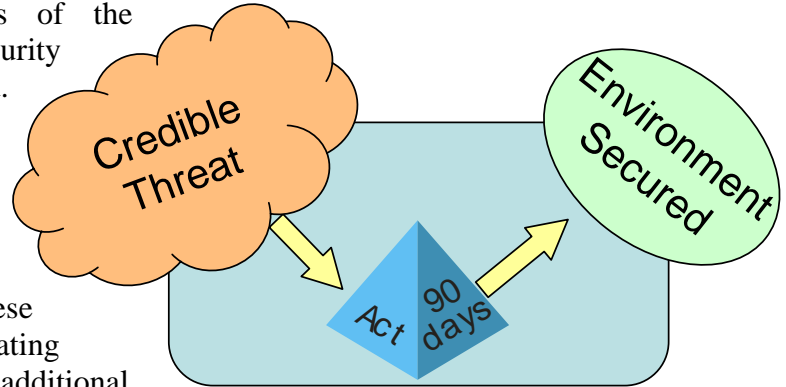


At this point it might be worthwhile to examine the corporations current and past information security practices to establish the historical foundation upon which we will build the next paradigm.

Background

Over the last 10 years, the security engineering team has been highly successful in addressing the security concerns of the enterprise. During this time, security engineering has steadily progressed. Initially, it utilized a highly-responsive threat-driven model.

Under this model, the engineering teams typically responded with solutions in 90 days. Many times these solutions were one-off fixes necessitating additional updates and/or presenting additional vulnerabilities.



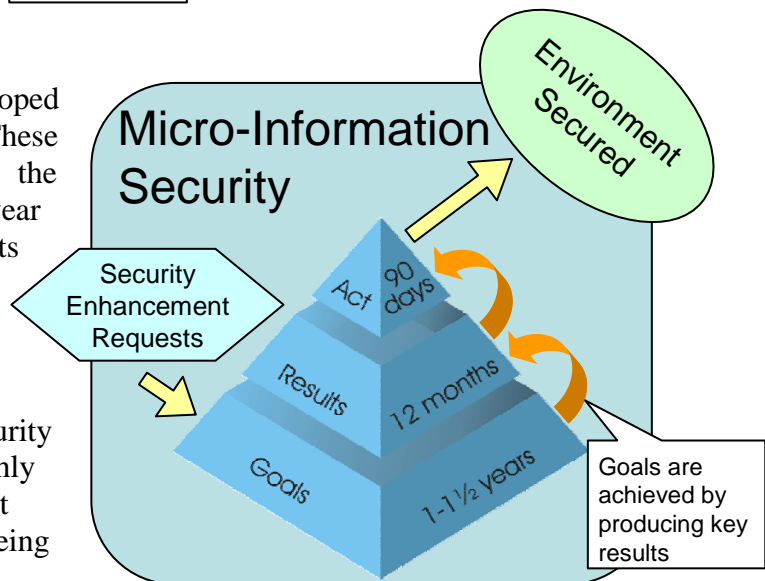
At the same time, security engineering was working diligently to address compliance issues. While equally complex, there was greater latitude in the timeframe to address these issues.

Corrective Action Plans (CAPs) were developed to address identified issues. These typically had a duration of 12 months and

were fully engineered solutions.

Finally, security engineering developed product roadmaps annually. These roadmaps served as establishing the target goals for the group in 1-1½ year timeslices. Typically, these requests were enhancements driven by the lines of business and/or the operations team.

Taken together, this has allowed security engineering and operations to be highly effective and successful. However, it has limited security engineering to being re-active to outside forces.



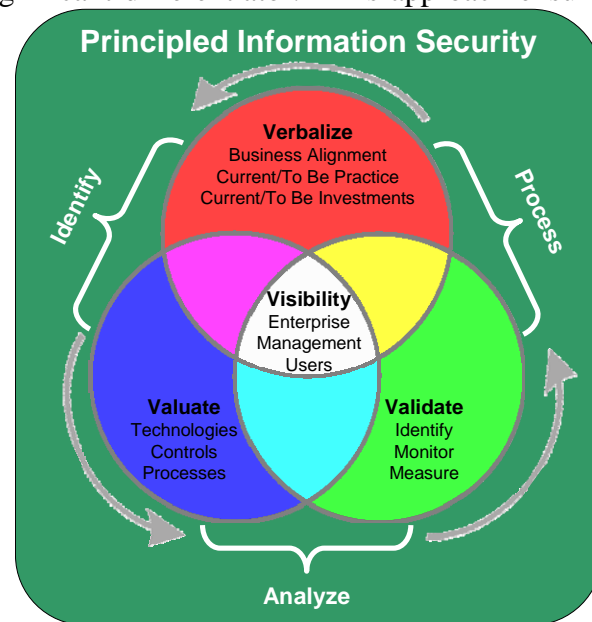
A paradigm shift is required for security to move from a re-active state and towards a proactive state. This shift can best be described as *Principled Information Security*.

Principled Information Security

Many of the corporation's information security professionals hold CISSP certifications. Ask them to define *information security* and they will faithfully recite the CISSP Information Security Tenants surrounding the Confidentiality, Integrity, and Availability of information. And that's OK, especially when having discussions among peers or when educating co-workers. However, they are probably not necessary for management presentations. Instead, information security can be conveyed as a *principled* approach, which may resonate better with management and non-security professionals.

The primary goal of principled information security is to raise information security's visibility to management such that it is considered for inclusion in all future business programs. This should not be limited to technology alone, but extended to business marketing and sales opportunities as a significant differentiator. This approach ensures success through the following principles:

- 1) Information security management, practices, and investments are verbalized in a manner that aligns with the business;
- 2) Controls, processes, and technologies are managed throughout their lifecycle to ensure the value proposition of the investment is sustained and possibly even enhanced;
- 3) Key investments are identified, monitored and measured on an ongoing basis for validation of their effectiveness.



Principled Information Security involves *Information Protection Stewards*, their programs, staff, and resources at the *onset* of every new business venture or project. It ensures up-front business alignment rather than after-the-fact input.

Information Protection Stewards

The concept and execution of information stewardship is nothing new within the corporation. We have recognized that our information assets are more than a valued corporate resource; it has significant value to entities outside our enterprise. Information stewardship, at its fundamental level is limited in scope to ensuring accountability. To this end, we have created Information Security Officers (ISO) and bestowed the title of Business ISO (BISO), Group ISO (GISO), and Technical ISO (TISO) on individuals for over a decade.

While the accountability of information use cannot be dismissed, the responsibility of protecting these assets – whether virtual, logical, or physical – is of the utmost importance. ISOs have become the de facto protection stewards in the company.

However, protection stewardship needs to extend beyond individuals with IT backgrounds and into the general enterprise in order to fully secure the constructs that enable our core business systems. Protection stewards include executive management,

legal, human resources, procurement, and any person or department handling information assets deemed vital to our ongoing operations and growth.

While education and training of our personnel has made strong inroads towards an understanding of each individuals' responsibility regarding protection stewardship, the bulk of effort has continued to fall on the information security professionals in the corporation to recommend and oversee the implementation of the controls and processes that protect us from cyber threats.

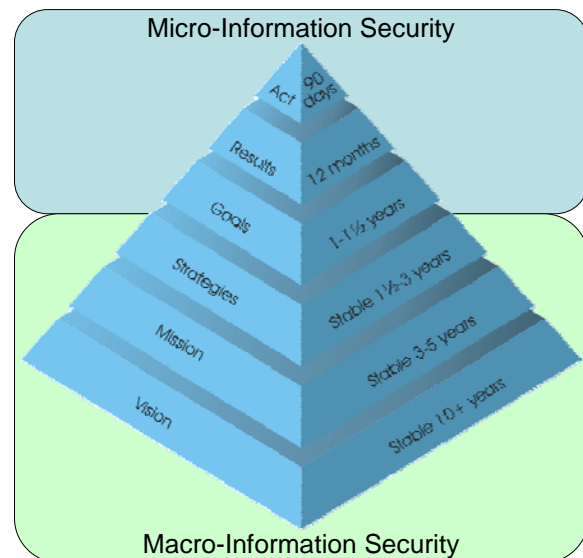
To be truly effective, protection stewardship needs to blend the tenets of information security, brand marketing, and business alignment. This presents a challenge, as most information security professionals in the company have a background in IT with a focus towards micro-information security. What is required is the paradigm shift towards the *principled information security* model. This may best be accomplished through the application of *macro-information security*.

Macro-Information Security

Economists figured long ago that in order to fully understand the economy, they would have to employ a two-pronged approach. The first approach would look at the economy by gathering data from individuals and companies on a small scale. The second would tackle the analysis of the economy as a whole. Thus was born micro and macro economics.

We can create an information security model that is better understood by borrowing from economics. By dividing information security in the same manner as economics, we get micro-information security and macro-information security.

Micro-information security is the reactive application of our technologies, controls and processes deployed on a day-to-day basis for defense against cyber threats. The corporate information security professionals have excelled at this and continue to provide world-class service. Where our security professionals could have more rigor is around business planning, i.e. *Macro-Information Security*.



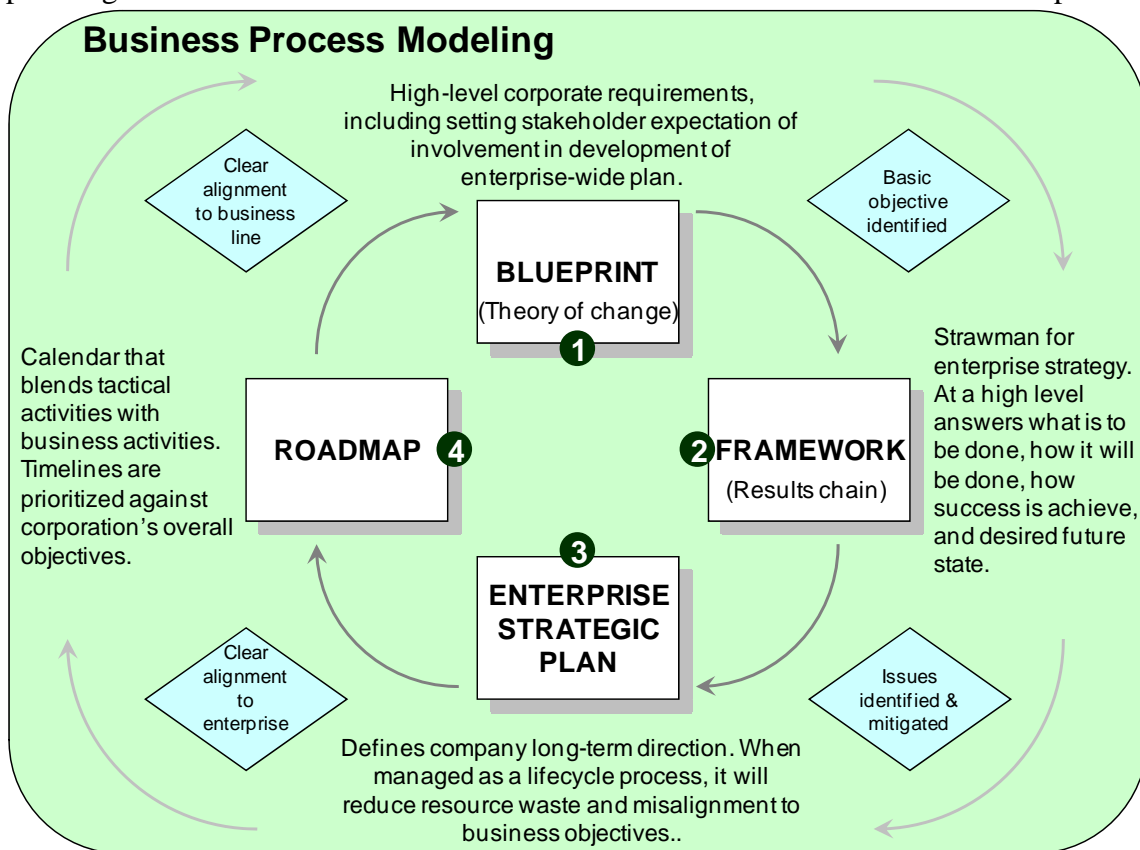
Macro-information security is the “*big picture*” that is designed to keep our executive management fully in the loop. It’s the stable strategic aspects of a multi-year plan designed to protect the enterprise while ensuring business alignment. It also extends externally to support our partners, customers and key vendors as well as ensuring compliance.

Macro-information security enables our security leadership to align the company’s security programs with the lines of business. It bridges *CISSP InfoSec-speak* with traditional business intelligence. When used correctly, macro-information security can be the tool that brings long-term success. And, success is being included in the planning stages for each new business venture, marketing campaign, or development project.

In order to plan strategically, our security architects, senior managers, engineering leads and operations managers must have an understanding of the business programs and objects that extends beyond IT. This understanding lends itself to the creation of concise and clear strategies and roadmaps that integrate security into the business sectors and show the value-add that information security can bring to the table, ultimately answering the question: “What is information security?”

Our business peers want to know the answer to this as well as why information security should truly matter to them. The typical business approach to answering this is through a strategic plan. However it can be tedious to focus on the technical details present in micro-information security roadmaps to those not well versed in IT and information security.

One method to address this and gain reasonable acceptance of a strategic security plan is to allow the business units to shape and mold the plan prior to it being formalized through an incremental, iterative process. Essentially, this means borrowing and applying traditional business process modeling techniques throughout the strategic security planning process.



1) Blueprint:

The goal is to gather enterprise-wide requirements, provide a visualization of those requirements, and continue the process of interweaving information security into the fabric of the corporate culture.

One approach is to utilize a *Theory of Change* logic model. Why? *Theory of Change* models stimulate critical thinking among stakeholders to identify early and intermediate accomplishments that will support sustained long-term change. These models help identify ways information security can provide positive impact to a business group, a sector, and/or the whole enterprise. Like any good planning and evaluation method for

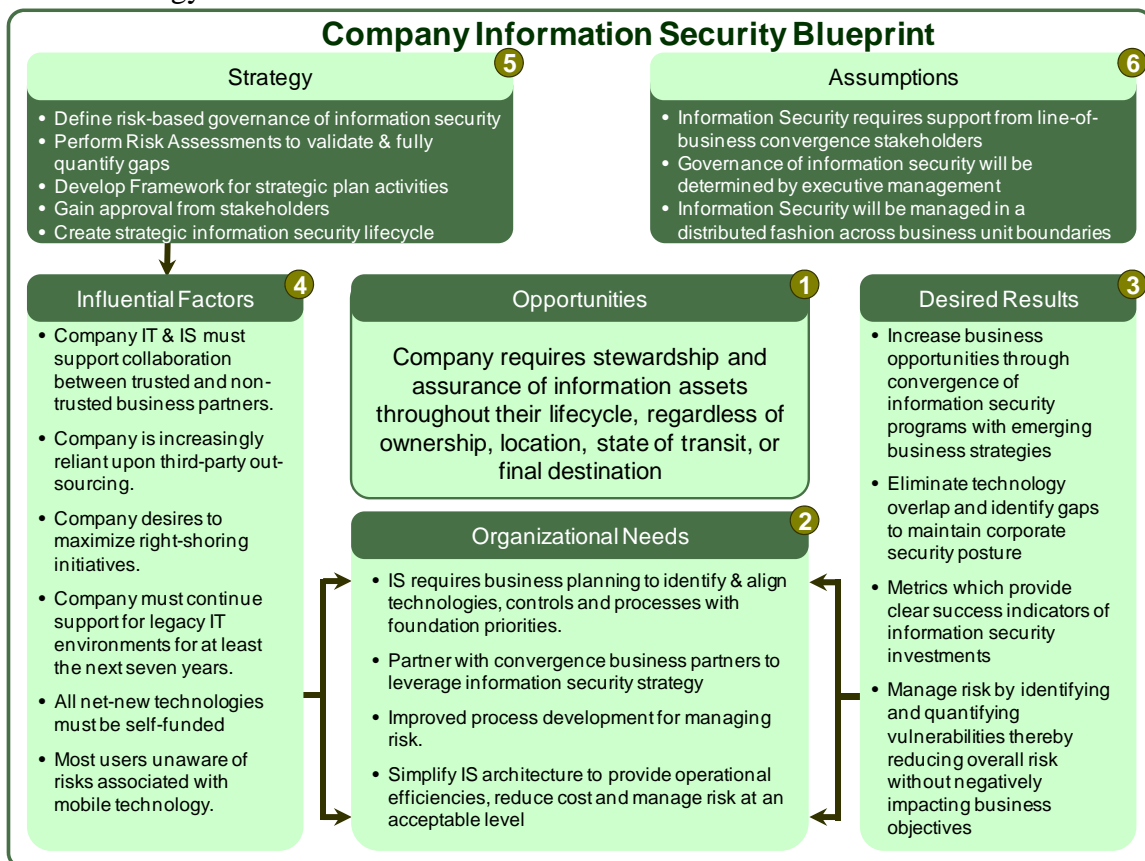
change, it requires participants to be clear on long-term goals, identify measurable indicators of success, and formulate actions to achieve goals.

It differs from any other method of describing initiatives in a few key ways:

- it shows a causal pathway from here to there by specifying what is needed for goals to be achieved.
- it requires us to articulate underlying assumptions which can be tested and measured.
- it changes the way of thinking about initiatives from what we are doing to *what we want to achieve* and starts there.

A *Theory of Change* model provides a high-level plan to get us from here to there. To do this, it should answer the following:

- 1) What do the lines of business, the sectors and enterprise require and what opportunities exist that can be addressed through information security?
- 2) What does the corporation need today?
- 3) What results should be reflected?
- 4) What factors will influence the success?
- 5) What strategic activities will be required to achieve desired results?
- 6) What conditions exist that are outside our zone of control that may affect the strategy?



Once the blueprint is completed, we will have re-defined information security in business terms at a very high level, engaged key business stakeholders, mapped out security priorities, and developed a long-term vision of information security within the company.

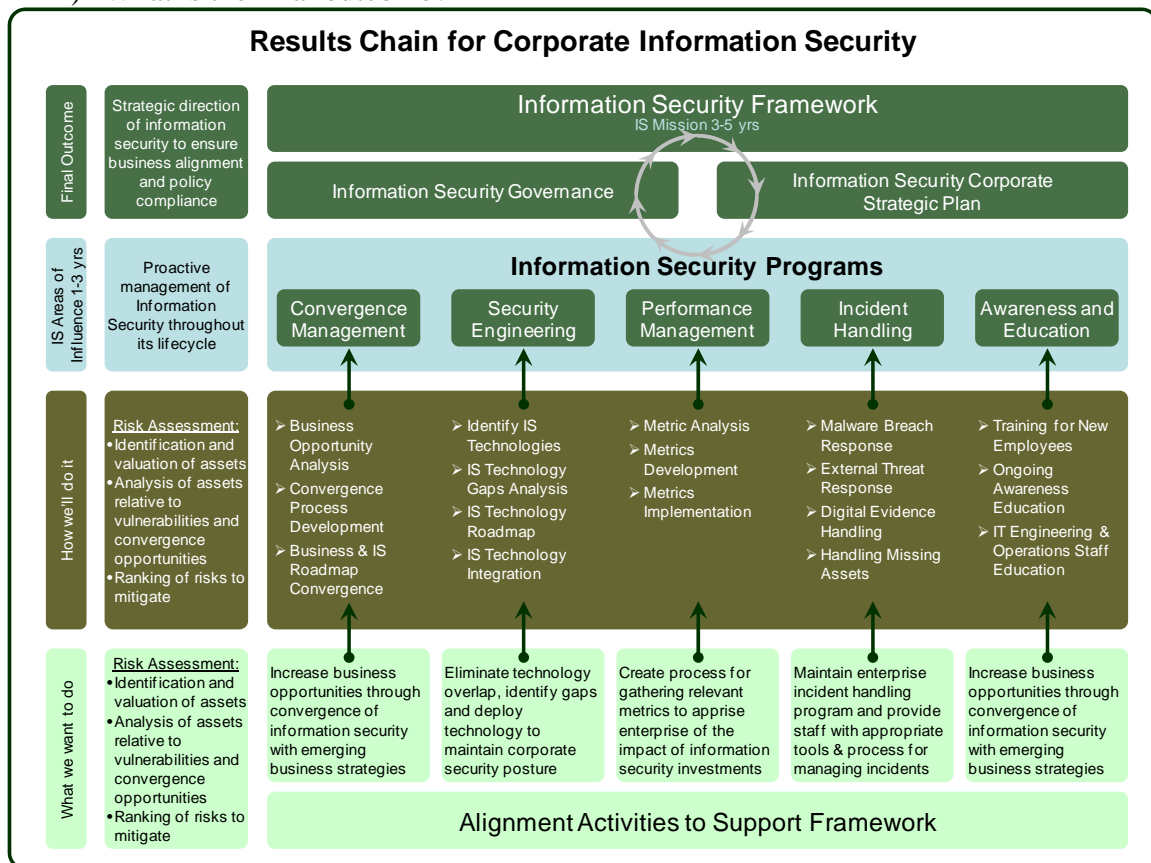
2) Framework:

The framework is based on the information gathered in the *Blueprint*. Use of a *Results Chain* logic model in building the framework allows us to clearly identify and present the high-level actions that will be taken to achieve the desired overall outcome. This five step process involves:

- I. Identify the driving forces/hindering forces impacting the vision conveyed in the Blueprint.
- II. Identify potential solutions and changes needed, generating a means-end model
- III. Analyze alternative strategies and prioritize results
- IV. Analyze conditions necessary for success – document risks and assumptions
- V. Develop indicators & identifying means of verification

Wider involvement at progressively lower levels within the organization is necessary to successfully build the framework as it is a comprehensive document. The *Results Chain* logic model provides a functional framework that answers these key high-level questions:

- 1) What do we want to do? What activities are required? This is a direct expansion of the results from the *Blueprint*.
- 2) How shall we do it?
- 3) What will be the rate of influence by years? This is a list of the major categories or programs that address what will be influenced.
- 4) What is the final outcome?



Completion of the framework yields a complete picture of the information security programs, the high-level activities necessary to build and sustain each program and identification of actionable goals. At this point it might be prudent to engage a third-party, such as Internal Audit, to perform a risk assessment, identify gaps, and validate the framework.

3) Strategic Plan:

The *Strategic Security Plan* defines the corporate information security's intermediate direction, encompassing 1½ – 3 year event horizon. When managed as part of a business planning lifecycle, it can reduce resource waste and misalignment to business objectives. The information gathered in producing the *Framework* will be used in the strategic plan as major milestones.

The body of the strategic plan contains the assemblies to be addressed. These are the targeted assemblies and the respective programs they roll up to, which were identified in the *Framework*. The assemblies are identified from the list of activities laid out in the framework document. Flowing from these targets are the components and projects necessary to achieve the targets.

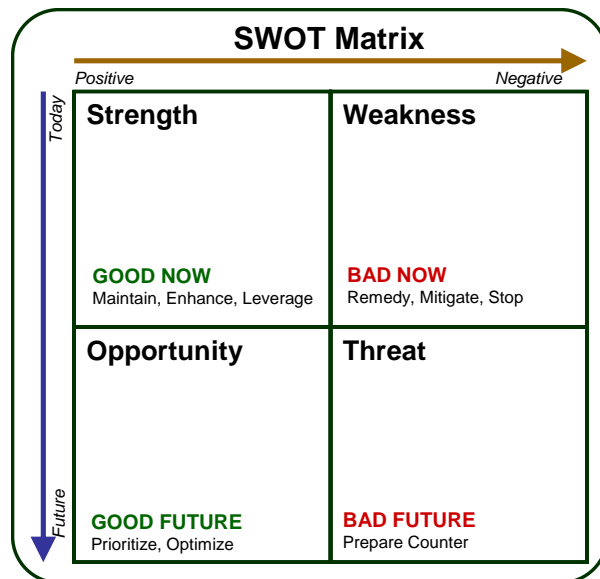
Additionally, the plan will contain elements such as cost, people resources, and challenges. All targets identified in the strategic plan must clearly map to and support the corporate vision for information security, as defined in the *Blueprint*. For each identified program, the strategic plan will answer:



- 1) Where are we today? This should include a description of the current environment and is pivotal to justifying the identified activities.
- 2) Where do we desire to be? This should include the identified targets, their associated costs and resources.
- 3) What barriers exist and what are the critical success factors?
- 4) What are the drivers?
- 5) How will the plan be monitored?

To gather the information necessary to address these questions an *environment scan* should be completed and the results charted on an SWOT (Strengths, Weaknesses, Opportunities, Threats) matrix. This gives a good visible reference to work from that when coupled with the *Blueprint & Framework* will allow for successful completion of the *Strategic Security Plan*.

Quite often the planers already know much of what needs to go into a strategic plan, especially if they have been involved in the *Blueprint & Framework* processes. However, development of the strategic plan greatly helps to clarify those plans and ensure key stakeholders are all on the same page. Far more important than the strategic plan document, is the strategic planning process itself.



4) Roadmap:

The strategic roadmap is the functional calendar that blends IS tactical activities with business activities over a multi-month calendar. Its timelines and delivery schedules have been prioritized by the findings of the SWOT matrix and aligned with identified business convergence opportunities. It is the path taken to satisfy the targets in the strategic plan. This is the cross-over point from stable macro-information security to actionable micro-information security and serves as one of the drivers for annual goal setting and project planning activities. At best, when viewed in conjunction with the *Blueprint*, *Framework*, and *Security Strategic Plan*, the strategic roadmap will be easily interpreted by leaders from the business lines and those who support technology.

Together, they will communicate without requiring further verbal narratives the value proposition of *Information Security*. At a minimum, the road map contains the targets, high-level activities, destinations, timelines, milestones and interdependencies.

Once completed, the Macro-Information Security model will answer the question “What value does *Information Security* provide me”.

