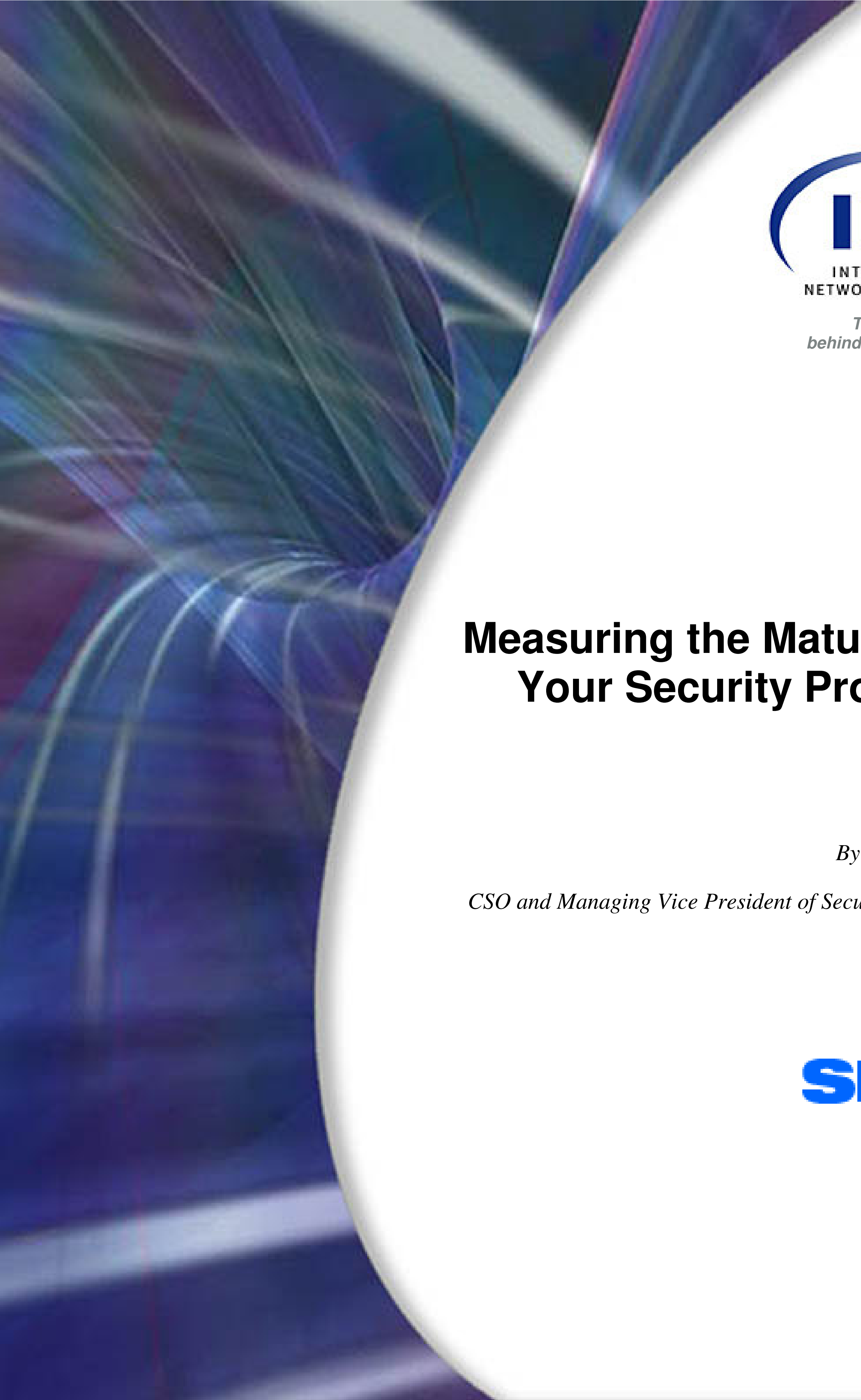


INS
INTERNATIONAL
NETWORK SERVICES

The knowledge
behind the network.®

Measuring the Maturity of Your Security Program

By Jim S. Tiller

CSO and Managing Vice President of Security Services

INS

SITA

Measuring the Maturity of Your Security Program

By Jim S. Tiller, CSO and Managing Vice President of Security Services

Introduction

Information security is a significant challenge facing the Travel and Transportation Industry (TTI). Combined with the relentless increasing sophistication of threats and reliance on information technology, many organizations are confronted with rigorous compliance requirements, adding a new dimension to how information security is visualized within the business environment.

It is well understood that managing a meaningful security posture requires due diligence and regular care and feeding. As adoption of IP/Internet-based technology by the TTI increased, point-solution security controls were incorporated to reduce risk and meet best practices. However, as time passed and information security became more important, it became increasingly clear that managing risk was more about a pragmatic, consistent, and repeatable methodology as opposed to fire-and-forget strategies.

Today, most organizations have employed a vast array of security technology and supporting documentation. Much of this is represented by firewalls, intrusion detection systems, anti-virus controls, security polices, and engineering standards. Although these practices satisfy the essentials of security, the maturity of the processes to support the security infrastructure directly correlates to the overall resilience, flexibility, and capability of the organization – all translating to the ability to manage risk over time and address challenges in an efficient manner.

This paper will demonstrate the importance of security program maturity, discuss the process of determining its effectiveness, and show how this will help you gain long-term valuation of your security investments.

Security is More Than a Box

Throughout the history of information security, many technical solutions have surfaced to help organizations address various security threats. Most notable was the introduction of the firewall, which by the late 90’s became a standard fitting at all Internet connections. Soon after, intrusion detection systems (IDS) became the next big wave of standard security technology. However, the avalanche of data on the state of network and system security activities provided by IDS overwhelmed many IT organizations. Consequently, processes and even additional technology were quickly introduced to manage the IDS and derive meaningful information from the data being obtained.

It was at this point that most realized optimizing their investment in IDS required processes to perform regular maintenance, monitoring, metrics, quality control, and, of course, experts to perform these functions. One could rightly argue that the investment in oversight far exceeded the hard costs of the technology.

Comprehension of the importance of process and its direct ties to ensuring realization of the investment in IDS ushered in a renaissance of information security, which is just beginning to take root.

Security Slippage

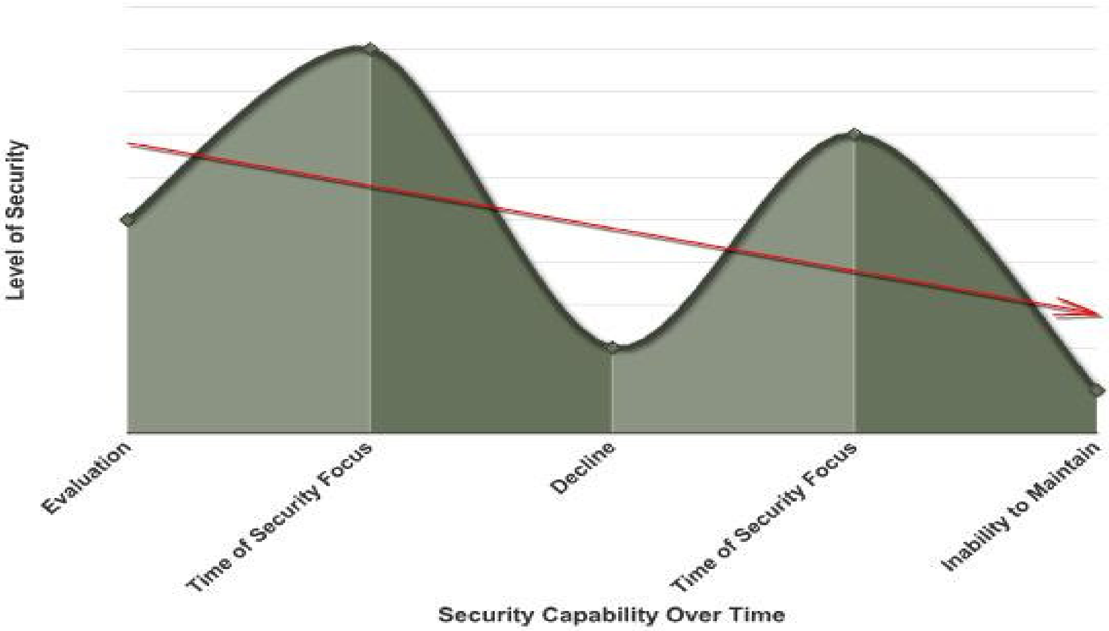
Given today’s knowledge of information security, most organizations have implemented standard security controls. These have materialized in the form of people, processes, and technology. Each element requires regular maintenance and governance or the organization will suffer from “slippage.” Fundamentally, slippage occurs when the security program lacks governance, which can be the result of lack of attention and focus, skilled resources, or investment, or simply unawareness that a problem is looming.

Traditionally, security controls wane over time and move into maintenance mode with no meaningful governance. Shortly thereafter, many solutions begin to fall victim to apathy. At some point during the decline an event occurs, such as an attack or business change, and once again security becomes the focus, resulting in more investment to increase the security posture.

The product of slippage is investment spikes, which disrupt budgetary cycles. Consequently, executives grow increasingly wary of this painful process, while their expectations for results decline rapidly. This repeating cycle hinders the ability of security to become a valuable participant in meeting the objectives of the organization.

Unfortunately, security posture tends to decline over time (Figure 1) unless a mechanism is employed to monitor the quality and capability of the information security management system.

Figure 1: Security Slippage Over Time



The only method for combating slippage is to identify problem areas before they become expensive gaps. This can be achieved by introducing a governance process that can interrogate the security program and provide a quality loop that ensures weaknesses in practices, skills, and technology are identified, adjusted accordingly, implemented, and validated.

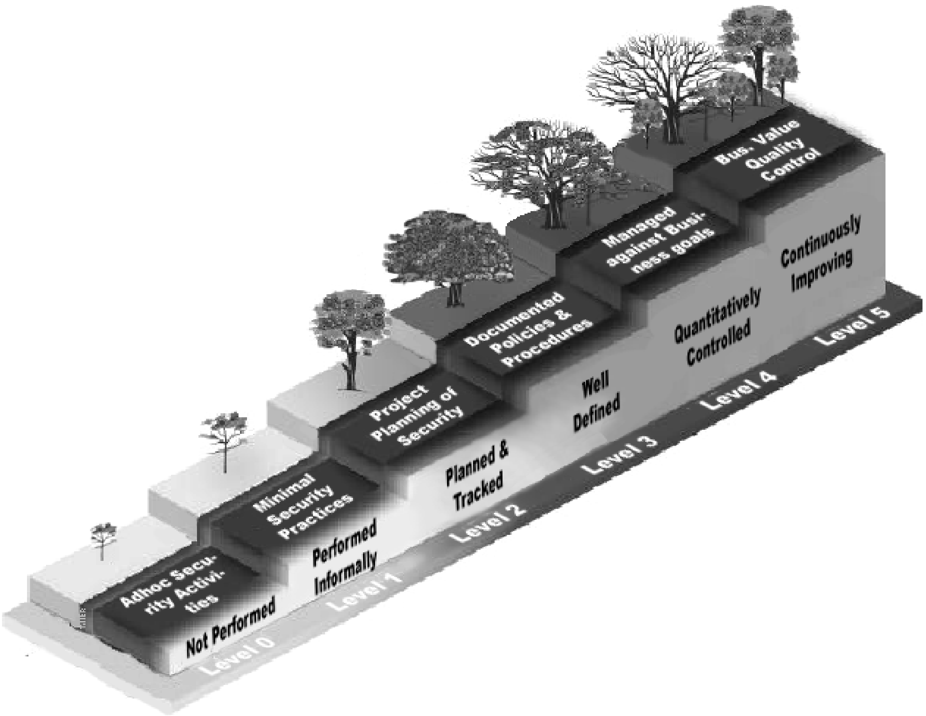
Security Maturity

The more mature security governance processes are, the more applicable security practices and technology are to the business. As the effectiveness increases or reaches a point that mirrors the organization’s desired security posture and risk profile, the greater the return on investment because the controls will last longer, have greater flexibility, and change can implemented quickly to address a business dynamic due to increased operational visibility.

There are several degrees of maturity, each representative of the sophistication of governance processes. There are a number of maturity models available, however one stands out: the System Security Engineering Capability Maturity Model (SSE-CMM), which can be accessed at www.sse-cmm.org. In 1995, Carnegie Mellon University created the Systems Engineering Capability Maturity Model. That model became the foundation for the SSE-CMM, as well as the INFOSEC Assessment Capability Maturity Model (IA-CMM), which the National Security Agency (NSA) uses to evaluate compliance and effectiveness of organizations using their INFOSEC Assessment and Evaluation Methodologies (IAM/IEM) with regards to the NSA's INFOSEC Assurance, Training, and Rating Program (www.iatrp.com).

In short, the SSE-CMM defines expectations of processes and capabilities for each level within the area of evaluation. At each higher level, SSE-CMM becomes less about a specific security attribute and more about the role of security within the organization.

Figure 2: Levels of Security Program Maturity


Adhoc Secu-rity Activi-ties
Not Performed
Level 0
Minimal Security Practices
Performed Informally
Level 1
Project Planning of Security
Planned & Tracked
Level 2
Documented Policies & Procedures
Well Defined
Level 3
Managed against Busi-ness goals
Quantitatively Controlled
Level 4
Bus. Value Quality Control
Continuously Improving
Level 5

The SSE-CMM presents five levels (beyond Level 0) of capability:

- Level 1
  - Base Practices are Performed - Focuses on whether a security organization performs a process that incorporates base practices. This is representative of the existence of security policies, system specific management practices, and security standards.

- Level 2
  - Planning Performance - Focuses on project-level definition, planning, and performance issues. This is where the organization begins to demonstrate the existence of oversight processes focused on the performance of people, process, and technology.

  - Disciplined Performance – Focuses on the existence of dedicated project management processes and documentation.
  - Verifying Performance – Focuses on the validation of actions and projects. Most attuned to the existence of a collection of processes and practices that are designed to investigate the effectiveness of controls relative to risk.
  - Tracking Performance – Focuses on the quality control processes related to specific projects, initiatives, or areas of security management. The goal is to determine if the organization has a quality process that establishes metrics of operations and maintenance, and the facility to incorporate change effectively.

- Level 3
  - Defining a Standard Process - Focuses on disciplined tailoring from defined processes at the organization level. This is representative of an overarching security governance process beyond an initiative, project, or domain.
  - Perform the Defined Process – Clearly, the existence of a process does not insinuate the process is being exercised accurately. This focuses on evidence that substantiates that the processes are being employed. For example, quality documentation, communications, action item registers, and deliverables.
  - Coordinate the Process – Focuses on the existence of processes and evidence, such as project plans and deliverables, that attest to the collaboration and alignment of practices.

- Level 4
  - Establishing Measurable Quality Goals - Focuses on measurements being tied to the business goals of the organization. Although it is essential to begin collecting and using basic project measures early, measurement and use of data is not expected organizationwide until the higher levels have been achieved.
  - Objectively Managing Performance – Focuses on the incorporation of measurements into the broader implications of meeting goals of the organization.

- Level 5
  - Improving Organizational Capability - Gains leverage from all the management practice improvements seen in the earlier levels, then emphasizes cultural shifts that will sustain the gains made. Level 5 is very difficult to achieve because it represents where security is supportive of business objectives and evidence of the fact. This can be likened to clearly articulating return on security investments (ROSI), which is significantly complicated given today’s operational and business strategies.

Given the complexity and sophistication that is required as the levels increase, organizations must approach the model from a pragmatic perspective. For example, if a company receives a score of 1.5 for a particular area of security, this does not suggest that the organization has failed in implementing the control, but rather represents the maturity of the supportive processes that ensure the control is properly maintained. Moreover, the organization is free to accept that level because it meets the needs of the business and desired security posture.

To gain as much value as possible from the process, it is critical for organizations to understand what level of maturity is acceptable for their needs. To achieve the next level in a capability maturity model it typical requires an exponentially increasing investment in the development and establishment of advanced processes. For some organizations this may simply be too great of an investment in the light of risk and the desired security posture. Therefore, a low score may be acceptable when balanced with the demands, desires, and constraints of the business.

However, it has been shown that the lack of maturity of security processes and governance represents the inability to sustain the security posture over time. As demonstrated previously, poor security governance translates to slippage and all that it implies. Ultimately, while organizations can avoid long-term investments by not adopting sophisticated processes, the minimalist-control strategy requires constant validation of existing controls due to the fact that slippage can occur much quicker

Security is a balance between managing business risk, investment strategies, and due diligence. It is up to the security organization to determine if the level of maturity of various security practices is in alignment with corporate objectives.

TrustCheck

In an effort to address the changing landscape of information security management and the desire of companies to understand the effectiveness of their security governance processes, INS in conjunction with SITA has developed a comprehensive security measurement solution called *TrustCheck*.

TrustCheck combines a custom developed evaluation tool, specific skills, and SITA-INS' NSA certified methodologies. By reviewing security documentation, processes, and evidence, and performing structured interviews, TrustCheck evaluates a security program to provide a perspective of maturity and capability.

First and foremost TrustCheck assumes that industry best practices are employed and, thus, is evaluating the governance of those best practices. If a control simply does not exist, a level of zero (0) is assigned, representing a fundamental gap. Secondly, TrustCheck takes into consideration when a component of the best practice is simply not applicable to the organization and removes the control from the calculation.

TrustCheck's framework is founded on modules. The concept is that the investigative process can be applied to any industry standard, regulation, or even internally defined standards and policies. For example, SITA-INS has developed modules specifically for ISO-17799, HIPAA, and Sarbanes-Oxley. For example, when investigating best practices, the ISO-17799 module can be used to guide the evaluation. If the organization is attempting to determine their adherence to a regulation TrustCheck can be used to reflect the existence and overall management of compliance efforts.

This combination of established analysis process based on SSE-CMM and modularity of the tool represents a significant departure from traditional assessments. The term "best practice" means different things to different industries, and even for different companies within the same market. Therefore, SITA-INS can produce an industry-specific module based on direct experiences in supporting security initiatives within any industry. Moreover, modules can be created for a specific company to investigate how well they are meeting their own established practices.

The value is in the fact that the NSA IAM-certified methodologies and SSE-CMM are simply frameworks of principles and devoid of specifications or prescriptions. To compensate, SITA-INS has developed a CMM Matrix for each module that defines the attributes that must exist for each level of the model. The CMM Matrix is a comprehensive list of requirements for each area of a given standard or requirement aligned to its framework. The matrix appears in two forms: 1) as supportive documentation within the methodologies, and 2) as statements incorporated for each investigative point.

For example, the ISO 17799:2005 module has roughly 600 investigative points (questions or statements) to guide the process. The process associated with each investigative point supports the collaboration between the investigator and the client. It also highlights the collection of specific documentation or evidence. Finally, each investigative point has a CMM Matrix component. As demonstrated in Table 1, the ISO 17799:2005 is broken into 11 domains; the first addresses security policies. Within each domain there are one or more elements with one or more subelements, which in turn contain the investigative points. As shown, the process focuses on determining whether the control exists and reflects the most fundamental best practice. The CMM Matrix element provides an overview of attributes that must exist to reach a given score.

Table 1: Example Module Framework

Element	Sub-element	Question/Statement	Process	CMM Matrix
Information Security Policy	Information Security Policy document	Has an information security policy document been approved by management, and published and communicated to all employees and relevant external parties?	Obtain and review the information security policy for accurateness and completeness. Obtain the approval form and process, validate existence, completeness, and that it has been appropriately employed. Verify employee communications and training.	The existence of complete policies and verifiable evidence of approval, communications, and training within the last year is optimal. More verifiable evidence, and the length of historical record relating to the sound management, communication, and training associated with policies increases the score. Any lack of basic evidence constitutes a maximum score of 2.

The per-point data is supportive of the larger collection of prescriptions in the module's overall CMM Matrix. To demonstrate the completeness of this approach, ISO 17799:2005 has approximately 600 investigative points, each with a process and CMM matrix statement. Moreover, the CMM Matrix defines 3-5 attributes for each level for roughly 132 subelements. That amounts to over 3,000 points of information that are used to accurately evaluate the maturity of processes that are in support of a company wishing to fully incorporate the ISO 17799:2005 security standard.

Though on the surface this seems highly complex and time consuming, in fact it is a very efficient process. For example, the investigative points are the basis of the evaluation, and using TrustCheck releases the investigator from excessive calculations. In addition, TrustCheck allows the incorporation of data from the assessment and uses it to produce the bulk of the deliverable. During the creation of the module, SITA-INS creates a base deliverable that provides the foundation of the evaluation, which includes helpful information about the activities and standards. When complete, the investigator incorporates all the findings and recommendations from the assessment and finalizes the documentation.

TrustCheck presents the data in form of a 0-100 score (i.e., 20 * level=score) to provide more granularity in the presentation of information. TrustCheck provides an overall representation of the score. As shown in Figure 3, the overall score is presented with the scores for each domain and the industry baseline determined by previous evaluations or other information collection processes, such as a detailed on-site survey. In the example, the organization's overall maturity is 2.7, which translates into a score of 54.7.

As with the overall score, TrustCheck provides for a detailed perspective of capabilities within each domain of the module. In Figure 4, the industry baseline and client maturity level is displayed against the system development and maintenance of the ISO standard. This allows a more granular level of interpretation of the findings.

Figure 3: Overall TrustCheck Score

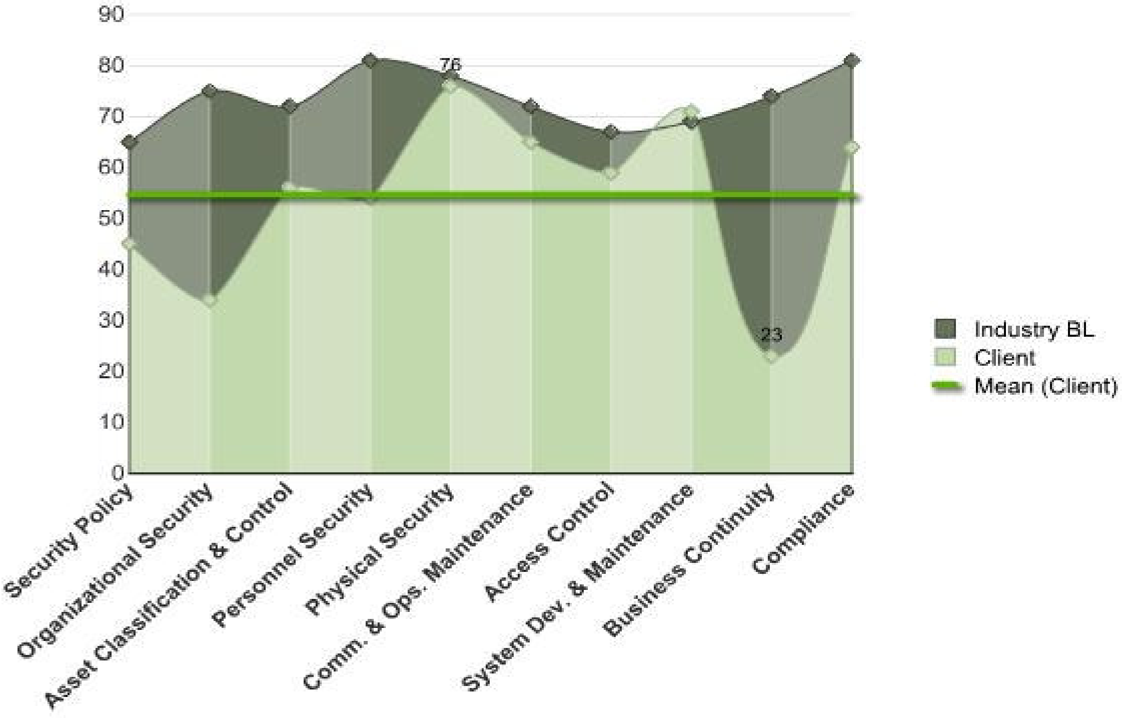
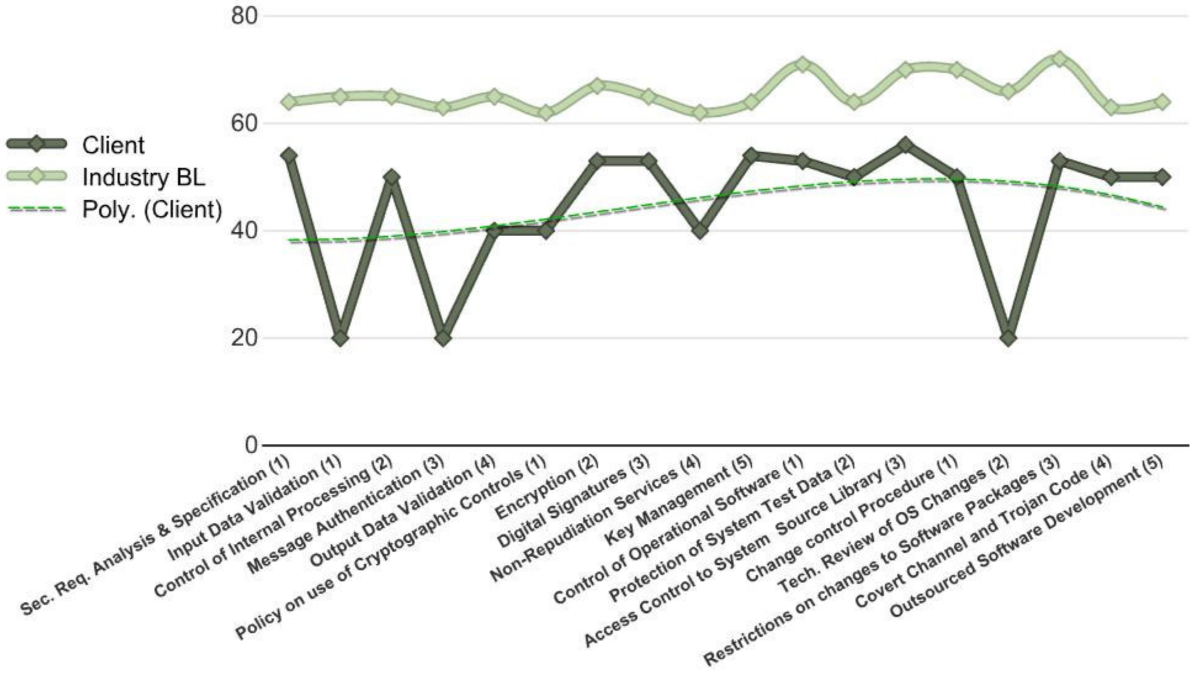


Figure 4: Example Domain Detail (System Development and Maintenance)



In addition to providing a visual representation of scores, TrustCheck produces a scorecard or a numerical representation of the information, furthering the data granularity. Finally, and most importantly, the deliverable contains a textual commentary on processes performed, findings, expression of existing security controls, and prioritized recommendations on how to leverage strengths and address weaknesses.

Setting the Standard

SITA-INS are in the process of executing a specialized TrustCheck module engineered for the TTI. The objective of this module is to obtain specific information about various information security practices shared by the industry as a whole. From this extensive effort, SITA-INS will have significant information to compile a meaningful perspective of the industry and create an acceptable and pragmatic security posture base-line. The results will include common recommendations, key strengths and weaknesses, and incorporate TTI best practices. This offers unparalleled value to the TrustCheck approach for the TTI.

In short, TrustCheck will provide exceptional visibility into the security program while comparing the findings to the industry baseline derived from the industry as a whole. The perspective of security capability will be matched to the findings of the industry with recommendations stemming from what others in the TTI are either performing as best practice or have accepted as a meaningful remediation tactic. This will allow organizations to understand their security condition, how they compare to the TTI, gain comfort in the recommendations, and have confidence in making informed decisions.

Therefore, TrustCheck is a unique application of processes, methodologies, and skills aligned directly with the TTI. Based on the development of a comprehensive survey of the industry, utilizing TrustCheck, a great deal of confidence can be realized. TTI organizations will gain a greater awareness of their security posture, a clear perspective of what others within the TTI are doing, and have all of the tools and information to address potential issues in a pragmatic and informed manner.

Conclusion

Many organizations have invested significant resources in meeting their security requirements and implementing best practices. However, as business perspectives and implications of information security mature, companies are seeking methods to gain the most from those investments and reduce gaps. The adoption of a capability maturity model to investigate the effectiveness of processes allows organizations to clearly visualize their current state and make informed investments in security with confidence in the outcome and its affect on the security posture.

Adopting a CMM also provides organizations consistency in measurement. To demonstrate growth and realization of investments, the evaluation methodology must remain constant, allowing the organization to recognize advantages in direct process improvements and indirect, tangential practice areas. Based on intangible attributes represented by culture and organic adoption of practices, investments in one area of security governance can have positive impacts on other areas. A consistent and proven evaluation process will support the identification of development derivatives enhancing other areas of the posture.

SITA-INS has recognized this need and has created a highly comprehensive solution that incorporates all the characteristics of a consistent, accurate, and efficient process.■

About INS

INS offers a comprehensive set of business and technology consulting services and software solutions to help organizations reduce operational risk, increase productivity, and support-revenue growth. Our **IT Infrastructure Consulting Services** deliver secure, business-centric infrastructures that integrate network, security, and storage technologies with best-practice operational frameworks. Our **Immedient Business Solutions** streamline and enhance business processes for enterprise project management and collaboration and analytics. And our **Diamond IP Software** provides flexible and scalable software solutions for managing today's complex IP networks. We have delivered tens of thousands of successful engagements worldwide over more than a decade of operation. INS is headquartered in Santa Clara, Calif., and has offices in the U.S., Europe, and SE Asia. For additional information, please contact INS at 1-888-767-2788 in the U.S., +44 1628 503000 in Europe, +65 6549 7188 Asia, or +1-408-330-2700 worldwide.

Further information can be found at www.ins.com.

About SITA

SITA SC is the only global Communication Services Integrator dedicated to the travel and transportation industry (TTI), providing consultancy in the design, deployment and management of complex communications solutions and reliably implementing, integrating and managing communication services. SITA SC is a commercially-managed not-for-profit organization, set up and wholly-owned by the air transport community. As a community of 600 airline and GDS members and 2,000 customers, SITA SC supports the TTI in driving down costs, removing complexity and improving operational performance. As a cooperative, any profit it generates is returned to its member customers. It is registered in Brussels.

Further information can be found at: www.sita.aero.