An Approach to Implementing Maturity Models in IT Security

Vasant Rao - Researcher
Rodger Jamieson - Director

SEAR: Security, E-Business, Assurance Research Group
School of Information Systems Technology and Management
University of New South Wales
e-mail: r.jamieson@unsw.edu.au

Abstract

This paper aims to study maturity models and how they can benefit organisations by developing a maturity model framework for IT security. The first part of the paper includes a discussion of maturity models and how they are applicable to the IT Security process and sets out the benefits of a maturity model approach to an organisation. The second part discusses examples of different maturity levels for different processes involved in the IT Security process. The paper concludes by comparing different maturity models in IT Security/Governance.

Keywords

Maturity Models, Framework, IT Security, IT Governance

INTRODUCTION

This paper uses an approach based on Maturity Models to create a framework to address the important issues of security and risk management. In our opinion, maturity models provides a structured approach to an issue like IT Security, which is continuously evolving. The paper firstly considers the history of maturity models and how they are applicable to IT Security. While maturity models themselves are not new, implementing a continuous improvement model for IT security presents a different set of problems. Next, an approach to maturity Models is suggested, followed by a discussion of how such an approach would be useful for organisations requiring a more continuous and strategic risk management.

HISTORY OF PROCESS MATURITY FRAMEWORK

The original concept for a process maturity framework was developed by Watts Humphrey and his colleagues at IBM in the early 1980s. In his 27 years at IBM, Humphrey noticed that the quality of a software product was directly related to the quality of the process used to develop it. Having observed the success of total quality management in other parts of industry, Humphrey wanted to install a Shewart-Deming improvement cycle (Plan-Do-Check-Act) into a software organisation as a way to continually improve its development processes (Deming 1986). Humphrey’s unique insight was that organisations had to eliminate implementation problems in a specific order if they were to create an environment that supported continuous improvement guided by Deming’s principles (Humphrey 1988).

The staged structure that underlies the maturity framework was first elaborated by Crosby (1979). Crosby’s quality management maturity grid describes five evolutionary stages in adopting quality practices in an organisation: the organisation would become aware of the new practice, learn more about it, try it in a pilot implementation, deploy it across the organisation, and achieve mastery in its use. This framework was adapted to the software process by Ron Radice and his colleagues working under the direction of Humphrey at IBM (Radice et al. 1985).

However, Humphrey realized organisations were not succeeding in long-term adoption of improved software development practices when they applied this maturity framework to individual practices or technologies. Humphrey identified serious impediments to long-term adoption that had to be eliminated if improved practices were to thrive in an organisation. Since many of these problems were deeply ingrained in an organisation’s culture, he realized an approach was needed that addressed the organisation, not just its individual processes. Consequently, he designed the process maturity framework to enable an organisation to achieve a state of
continuous process improvement via five stages, which became the main inspiration of modern day maturity models (Humphrey 1995).

On the information security front, early management techniques were in the form of a checklist-standard-based methodology securing software or information systems (Baskerville 1988). Even though checklists are no longer a hot topic in the contemporary information security industry, their cognate method – security management standards are increasingly getting more focus (Rasmussen 2000). Both checklists and management standards offer a ready-made generic catalogue of controls (Baskerville et al. 2002) and other protection means, which have been documented through the culmination of years of experiences of IS security practitioners. These standards define the set of evidence, sufficient for different ratings under the security criteria to define the ‘assurance requirements’ (Wichers et al. 1994).

Following ideas and developments in the field of software engineering, a few information security management practitioners started to apply principles of maturity models to information systems security (Ferraiolo et al. 1993). In fact, the major difference between information security maturity criteria and checklist-management standards is the concept of ‘maturity levels’ with the emphasis on learning and improving from past experience. As Siponen (2002) puts it, “any information security checklist or management standard can be turned into a maturity criterion simply by dividing the checklist or management standard into maturity levels”. However, organisations are starting to understand that compliance with security guidelines by completing a checklist with all ‘Yes’ marked, does not mean that they are ‘completely secure’ (WISSSR 2001). Jelen et al. (1998, p1) believe that “it is becoming increasingly difficult to gain and communicate assurance. As the level of interconnection and complexity in products and systems increases, the amount of information required to justify even the simplest claims grows quickly. Simple lists of evidence requirements are not adequate to represent the information required to represent assurance.”

Organisations need to constantly update themselves regarding new threats and vulnerabilities, while at the same time be more efficient by learning from the past. Thus, having ‘secured’ the current set of problems, organisations should incrementally secure emerging issues, effectively building on the security process. Maturity models advocate such a continuous improvement framework compared with a process standard comprising of best practices. The model integrates improved practices into a staged process that enables an organisation, (through a series of cultural transformations, each of which supports the development of more sophisticated and mature development processes) to provide a continuous basis for the risk management process.

With this background, the paper proposes a new approach to implementing IT Security using a continuous improvement model. The new approach was designed by conducting a critical comparative analysis of different IT security management maturity models existing in literature - refer Appendix 1.

THE FRAMEWORK

Maturity models for controls over IT processes consist of developing a method of scoring so that an organisation can grade itself from a non-existent level of controls to efficiently managing its processes. The model provides the stages through which processes progress as they are defined, implemented and improved. The framework provides a guide for selecting process improvement strategies by determining the current capabilities of specific processes and identifying the issues most critical to process improvement within a particular domain. A maturity model takes the form of a reference model to be used as a guide for developing and improving a mature and defined process to achieve certain goals.

The maturity process is best understood if the measurement process is associated in terms of a ‘scale’ (Jelen et al. 1998). This scale could employ numeric or qualitative values, or alternately it could be absolute or relative. For example, one might define ‘security need’ as limiting annual loss expectancy from some cause to less than $100,000, or as restricting the extent of data corrupted by a virus to an amount no greater than that from user error. However, whether our statement of need is expressed in absolute (first example) or in relative terms (latter example), it ultimately requires a means and a scale of measurement. Determining whether or not virus-caused data corruption exceeds that from user error presumes some way of measuring both. Once a measurement scale is selected, the ‘security need’ (goal) can be expressed as a threshold value on that scale and a measurement of the actual level can be made. A comparison of the two values will provide a judgement of the present situation. Whether the security goal is satisfied will depend upon the overall context which takes into account all the parameters involved in defining that goal. The use of maturity models greatly simplifies this process by providing a pragmatic and structured approach for measuring how well developed the processes are against a consistent and easy-to-understand scale.

The developmental nature of a maturity model means that process maturation is cumulative. Lower stage processes provide the foundation for upper stage processes. As additional critical processes are introduced into the organisation and implemented, the organisation attains greater process capabilities and the ability to achieve
higher level goals. The maturity progression also means that as the organisation incorporates additional processes at each successive stage of maturity, previously implemented lower stage critical processes must be maintained.

The maturity framework assumes that each practice has a risk to its successful adoption that is directly related to the maturity of the organisation’s existing base of practices. One important premise of the model is that sophisticated practices should not be attempted until the foundation of practices required to support them has been implemented. Thus, the practices at each level of maturity prepare the organisation for adopting practices at the next level. This staging of process maturity levels is unique in the organisational change literature and provides much of the framework’s power for improving organisations.

THE NEW APPROACH

Today’s systems, and the enterprises in which they reside, are so complex that even the most capable risk measurement tools are unlikely to yield risk values that are much better than rough indications of relative risk – which in most cases is often quite good enough. The problem is that the value of risk, whatever it turns out to be, is likely to be surrounded by a fairly large but unknown amount of uncertainty. This can create a dilemma for the decision-maker who must then decide whether to invest in further safeguards, which will undoubtedly reduce the overall risk but could be both expensive and unnecessary, or to collect more evidence to reduce the amount of uncertainty surrounding the effectiveness of the assurance process (Berinato 2002).

As cited above, there exists many security management guidelines in the market today. In one way or the other, any security guideline will acknowledge the need for security awareness among the employees and advocate appropriate education and training for all users and administrators. Broad level statements like these, while easy to formulate, can be ambiguous. Does the term ‘awareness’ refer to being aware of something (security), or refer to a state of affairs where employees are fully committed to the security policy. That is, it is very easy to measure the numbers of trained individuals; but measuring the effectiveness of the training or the appropriateness of training materials is extremely difficult.

Such ambiguity results in ‘reference-only’ practices that do not provide any guidance on how management can know with confidence that employees are aware of, or committed to, security policies and procedures adopted by the organisation. The problem is therefore, that unless one has a way to specify security needs in some measurable way, management cannot say with confidence with the security needs have been satisfied. Williams et al. (1998, p1) reminds us that “the whole security paradigm revolves around determining what ‘security needs’ are, whether or not they have been ‘satisfied’, and how to determine ‘confidence’ that we are fulfilling the security needs (goals)”.

With this viewpoint, we hypothesise that organisational maturity may be broken down into three broad categories (refer Figure 1):

1. Processes – activities which define the information system engineering practices, which include both management as well as technical processes.
2. Assurance – activities which give or inspire confidence in the whole process.
3. Metrics – indicators which provide qualitative as well as quantitative information related to the above activities.

![Figure 1: The three-dimension framework to organisational maturity](image-url)

To elaborate, processes are the activities performed directly to ‘secure’ the organisations and its related functions. This can range from management activities such as conducting a Threats-Vulnerability Analysis...
(TVA) to technical security (e.g. installing a firewall). The second dimension of assurance provides the basis for confidence that the security measures (technical, management or operational) work as intended to protect the system and the information it processes. An example of such assurance can be provided by say complying to the ISO 17799 standard. Stoneburner (2001, p3) advises that “Assurance provides a check that the security objectives of the organisation (e.g. integrity of transaction, availability of resources, confidentiality of information) have been addressed by a specific implementation when:

- required functionality is present and correctly implemented,
- there is sufficient protection against unintentional errors (by users or software), and
- there is sufficient resistance to intentional penetration or by-pass”.

But on its own, assurance only provides baseline confidence in the security process. It is not enough unless the organisation knows the performance level of the different processes and the related controls. This gap is filled by the third dimension. Metrics provides the necessary measurement step to the assurance process, measuring the efficiency, effectiveness and the impact of the security process. This in turn gives the organisation valuable knowledge to better the security process, which forms the basis of the continuous improvement paradigm.

A critical feature of the view presented above is that the three different dimensions complement each other and the overall organisational maturity is a cumulation of the other dimensions. Keeping these dimensions separate helps to establish a clear distinction between them and thus reduces the confusion caused by any overlapping of their meanings. For example, confusing the assurance dimension with security processes (practices) and metrics dimension makes it very easy to miss interesting cases where the three dimensions lead to conflicting conclusions.

To illustrate, consider an Anti-Virus (AV) system which is installed on the corporate server to curb the increasing number of virus incidents attacking the organisation. Now if this organisation is audited according to say the ISO 17799 standard on Information Security Management (ISO17799 2000) – the satisfaction of the control statement Section 4.6.3 on malicious software from the guideline, ‘Detection and prevention controls to protect against malicious software shall be implemented’ will technically comply with the requirement that the organisation should provide suitable controls to protect the integrity of software and information. But is the organisation confident that the goal behind installing the AV system is fully satisfied? It is unclear whether the AV system achieves the said objective comprehensively since there is no effective measurement to give us the degree of success or confidence. To continue the example, consider the case where after installing the AV systems there is a reduction in the number of virus incidents. Unless there is a well-defined system of metrics associated with the AV system, there is no guarantee that the reduction of incidents is due to the AV system - it could be the case that coincidentally the number of virus attacks decreased. Now consider the case where the number of incidents increases. In this case, management will be discouraged that the controls are not working and in spite of investing in technology they are not getting the results. It is technical requirement that the success of the AV system will depend on the administrator or the user updating the virus profiles on a regular basis. If this task is not performed, the AV system is not going to be effective. The point being stressed here is that a narrow focus on only the process (installing the AV system) and its related goal (reducing the number of incidents) do not provide the complete picture. A broader viewpoint is required in terms of metrics – that is how many viruses are hitting the AV system, how many were detected (and stopped), how many were not detected, why were these not detected. And finally assurance related to whether the goals are being defined properly, whether the metrics are answering these goals, is there ‘evidence’ in terms of demonstrated practice to substantiate the arguments. Without the complete picture, it will be difficult to attribute success or failure to any process.

In short, the three dimensions – processes, assurance and measurement alone do not provide the success associated with out goals. The three processes while independent provide a basis of feedback to the other, forming a balance of activities which in turn provides for improvement. At the same, these three dimensions complement each other by providing the necessary questions/arguments which will need to be answered (via evidence) to fully achieve our goals with the highest degree of confidence.

**WHY MEASURE**

We measure because we need to know about an attribute or characteristic of something that is important to us. In other words, measurements provide a single-point-in-time view of specific, discrete factors which can be alternately related to the process of counting. A metric on the other hand is a vehicle for understanding, by providing a standard unit to be used as a basis for comparison among like items or characteristics to enable decision making. In the same way, control metrics enable organisations to assess their process capabilities that are needed for understanding and evaluating the development and maintenance processes (Pfleeger 1995). Metrics are derived by comparing to a predetermined baseline or to two or more measurements taken over time.
An information security metric is formally defined as – a value, selected from a partially ordered set by some assessment process, that represents an security-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence (WISSSR 2001). Vaughn (2001, p3) expresses his view that “Security metrics focus on the actions (and results of those actions) that organisations take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defences are breached”.

One way that metrics promote understanding is by making aspects of development or maintenance more visible. This enables us to see into the ways in which processes, products, resources, methods, and technologies relate to one another. In addition, metrics allow participants in the process to define a baseline for understanding the nature and impact of proposed changes. Aided by metrics, we can answer questions not only about measuring process improvement, but also justifying security expenditures, monitoring and objectively documenting the organisation’s security posture, discovering areas needing correction, and establishing security goals (Kormos et al. 1999). Finally, metrics allow both managers and developers to monitor the effects of activities and changes on all aspects of development, so that action can be taken as early as possible to control the final outcome should actual measurements differ significantly from plans.

Thus, measurement is useful for:

- visibility and understanding (e.g. business value gained or lost from the security related activity);
- establishing a baseline for improvement (e.g. understanding the level of implementation of its own security standards, policies, and procedures); and
- planning, monitoring and controlling products, processes and resources (e.g. determining the effectiveness of the standards in protecting the enterprise, based on the results of their implementation (Pfleeger 1995), (Bartol 2001).

Although a measurement program is an essential part of any development program, it is useful only in the larger context of assessment and improvement. Choosing metrics, collecting data, analysing the results, and taking appropriate action require time and resources; these activities make sense only if they are directed at specific improvement goals. Thus the maturity framework is designed for application to practices that contribute directly to the business performance of an organisation. Implementing a value-generating measurement program requires that attention be given to the proper mapping of some identifiable organisational goal onto the measurement program, and a translation back of measurement results to organisational actions (Niessink et al. 2001). Realising this, the process maturity framework is used to ensure that what needs to be measured is visible in the process, which in turn helps management understand the relationships among the processes, metrics and the goals to determine the key opportunities for immediate improvements (Pfleeger 1995).

**CONTINUOUS LEARNING AND IMPROVEMENT**

Some processes are more mature than others, in that some processes are open and easily controlled, whereas others are arcane and dependent on a small set of process managers. A key discriminator among process maturity levels is the amount of visibility managers have into the overall process engineering and control process. At the lowest level of maturity, the process is not well understood at all; as maturity increases, the process is better understood and therefore better defined.

According to Basili and Rombach, “... (Improvement is only possible if we  
  a) understand what the current status of our environment is  
  b) state precise improvement goals for the particular project and quantify them for the purpose of control  
  c) choose the appropriate process execution models, methods, and tools in order to achieve these improvement goals, execute and monitor the project performance thoroughly  
  d) provide a feedback mechanism – analyse the data to evaluate the current practices, record the findings, determine problems, investigate alternate strategies or solution and finally make recommendations for improvements.” ((Basili et al. 1988, p 761)

Maturity models can provide such a framework for the characterisation, planning, construction, analysis, learning and feedback tasks. The key is to provide a systematic approach for setting project goals (tailored to the specific needs of an organisation) and defining them in an operational and tractable way. Goals are then refined into a set of success factors, the success of which will depend on a set of metrics for the different processes. And to complete the framework, ‘evidence’ to prove that the goals have been successfully met can provide the confidence or assurance factor. This whole process can be practiced on a cumulative basis so that the organisation is continuously learning and improving as shown in Table 1.

The critical element being stressed in the above discussion is the use of metrics in a maturity models framework. The process of defining goals, success factors or providing evidence each involves metrics. Maturity models...
which advocate metrics as part of their process will differentiate from conventional security management guidelines which indirectly insist only on the use of existing and well-known methods and practices. Information systems security today not only involves technical and business level considerations but also social as well as environmental issues, which are highly unpredictable. Security managers will therefore have to constantly find new ways to deal with unpredictable risks since a general prescriptive model will not suffice to deal with new threats in the market. By defining metrics, for example critical success factors for the processes which are of concern to the organisation, the security manager can then track these in time to find out exactly how the processes are performing and depending on the outputs the manager can take suitable steps which will lead to a more secure system. Maturity models can therefore encourage ‘innovation’ in trying to achieve the goals set by the organisation depending on its culture and environment as compared to just satisfying an all purpose security guideline which only prescribe broad based criteria2.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad hoc approach to process and practice</td>
<td>Processes follow a regular pattern</td>
<td>Practices are defined, standardised and documented</td>
<td>Internal best practices are applied</td>
<td>Best external practices performed through industry feedback and analysis</td>
<td></td>
</tr>
<tr>
<td>No review or audit performed</td>
<td>Monitoring only in critical areas of concern</td>
<td>Security compliance audit using industry baseline standards</td>
<td>Comprehensive Risk Management involving both technical and business managers</td>
<td>Organisation regularly participates in industry benchmarking</td>
<td></td>
</tr>
<tr>
<td>No defined metrics</td>
<td>Basic process related security metrics established</td>
<td>Metrics established with defined goals are analysed for feedback to improve processes.</td>
<td>Metrics designed with business focus (e.g. use of Balanced Score Cards)</td>
<td>Balanced Scorecards techniques and other scoring tools used extensively to provide continuous assurance and optimise processes.</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Continuous improvement based on the 3 dimensions

BENCHMARKING

The advantage of a maturity model approach is that it is relatively easy for management to place themselves on a scale and appreciate what is involved if they need to improve performance. Because they are management processes, increased maturity and capability is also synonymous with increased risk management and increased efficiency. In an age of increasing electronic business and technology dependence, organisations will have to demonstrably attain increasing levels of security and control. Every organisation must understand its own performance and must measure its progress. Organisations need to be able to determine the level of adherence to the control objectives either through a quick self-assessment (Kormos, 1999) or as a reference in conjunction with an independent review.

Management may wish to put in context any of these assessments, by comparison to the industry and environment they are in. Such comparisons can provide a strategic reference point for an organisation to improve security and control, which in turn could also consist of looking at emerging international standards and best-in-class practices. The emerging practices of today may then become the expected level of performance of tomorrow and are therefore useful for planning where an organisation wants to be over time. Benchmarking and measuring progress against peers and the enterprise strategy is one way of achieving a competitive level of IT security and control.

To satisfy this need, the IT Governance Institute3 in collaboration with Information Systems Audit and Control Association (ISACA) has put forward an open standard called COBIT (Control Objectives for Information Technology), which deals with IT Security as a part of the IT Governance control objectives. As a part of its management guidelines, COBIT provides a generic maturity model (seeFigure 2) with an incremental measurement scale – based on a rating of ‘0’ through ‘5’ (COBIT-MG 2000).

While scoring organisations on their maturity levels through a benchmarking process can benefit organisations by understanding the ‘state of play’ – without proper understanding and implementing controls, organisations can overrate their level of maturity as good maturity ratings could result in good publicity and an increase in business competence (Bollinger et al. 1991). While the study concentrated on software maturity models, the

---

2 The intention here is not to say that maturity models should replace information security management guidelines. Information security guidelines are definitely needed as a baseline of minimum criteria from which maturity models can build on depending on the needs of the organisation. They also provide a good starting point for organisations wanting to ‘secure’ themselves quickly.

3 http://www.itgi.org

Rao, Jamieson (Paper #265)
suggested countermeasures to deal with this problem [like including conducting online empirical evaluations (not just paper-based), requiring two sources of confirmation, and choosing a representative evaluation team] are also applicable to IS security maturity models as well. These countermeasures are direct examples of the assurance dimension. However, O’Connell et al. (2000) study revealed that these proposed cures in isolation did not totally remove the problem of distorting the truth. A crucial aim of setting up information security maturity criteria is to assist other organisations, third parties, business partners, etc. to ensure that organisations which they deal with have a certain level of information security. Unless there is a focus on demonstrated practice and performance evaluation, real improvement will be difficult (Siponen 2002). For this reason CobiT advocates the use of business oriented metrics like Critical Success Factors, Key Performance Indicators, Key Goal Indicators to look at the bigger picture, that is to measure the different processes and how they perform in terms of not only the technical needs but also in terms of the business goals (COBIT-MG 2000).

Figure 2: The CobiTgeneric maturity model (Source: COBIT Management Guidelines, ISACF)

Maturity models with such an approach will help professionals explain to managers where IT management shortcomings exist and set targets for where they need to be by comparing their organisation’s control practices to best practice examples. The right maturity level will be influenced by the enterprise’s business objectives and operating environment. Specifically, the level of control maturity will depend on the enterprise’s dependence on IT, the technology sophistication and, most importantly, the value of its information.

CONCLUSION

The importance of information security is paramount in today’s uncertain environment. While the issue of information security management is not new, organisations are facing a tough proposition of securing themselves in the constantly increasing risk environment. To help organisations, many guidelines have been published in the past – but these guidelines are proving to be limited in their approach due to their static nature, as compliance to the guidelines are basically at a point-in-time. Organisations need more than this to address risk management on a more continuous basis. This paper has discussed a maturity model to implement a ‘culture of security’ (OECD 2002) within organisations on a continuous basis over the long term.

As highlighted in the paper, maturity models are not new and have been successfully implemented in organisations developing software with very good results. If implemented correctly, similar benefits are possible for organisations wishing to ‘secure” themselves. The main focus of this paper has been on the implementation of maturity models. The approach discussed essentially combines the benefits and advantages of guidelines with a metrics driven approach to define a continuous model for improvement. While such an approach has been implicitly followed by most maturity models in the market, this paper highlights the advantage of distinguishing the issues of processes, assurance on the controls and metrics for feedback, analysis and decision making. This distinction helps to understand maturity models better and make their implementation easier – providing organisations with a roadmap to strategically deal with risk and security. Our framework also provides a springboard for further research.

REFERENCES


<table>
<thead>
<tr>
<th>Processes</th>
<th>Assurance</th>
<th>Metrics</th>
</tr>
</thead>
</table>
| **Information security program maturity grid (Timothy Stacey)** | Security is divided into 5 broad level process domains:  
- Mgmt understanding and attitude  
- Security organisation status  
- Incident Handling  
- Security Economics  
- Security Improvement Actions | Arguments grouped under an incremental model consisting of 5 stages:  
I. Uncertainty  
II. Awakening  
III. Enlightenment  
IV. Wisdom  
V. Benevolence  
Each of the above stages, there is a description of different criteria applicable across the process domains. In addition, the model describes the requirements to be satisfied for going from a lower stage to a higher one. The framework places low emphasis on ‘evidence’ requirements to substantiate the claims that the criteria has been satisfied. | While there were NO pre-defined metrics applicable across the process domains associated with the model, implicit financial measures like ‘Prevention Costs’ & ‘Loss’ amounts (under Security Economics domain) have been advocated at the different incremental stages to track the cost (success) of the security program. |

| Decision Support Metrics Framework (Ralph Leighton) | The framework prescribes a metrics driven incremental approach to security. Only examples of different aspects of IT security from a technical perspective (e.g. Vulnerability assessment, Penetration testing) are discussed throughout the framework. | The framework does NOT place much importance on assurance except at the later stages. E.g. compliance and verification is only considered at Stage III. The framework does not describe any criteria statements to judge the successful achievement of a particular level. | A 5 phased metrics driven approach to security is advocated with each phase presenting unique requirements for the establishment of metrics.  
I. Quick-fix  
II. Architectural  
III. Compliance  
IV. Adjustment  
V. Testing  
In the view of the author, “each of the phases produces measurable results that immediately and continuously benefit the organisation and that establish a foundation for the next step.” |

| Gartner’s Security Process Maturity Model (Gartner Research) | IT security divided into 7 broad level domains (management as well as technical) with each domain consisting of the different sub-areas of focus:  
- Business Perception  
- Security Budget (organisation)  
- Security Budget Spending (What the money spent on)  
- Technologies and Tools implemented  
- Security Organisations  
- Transaction Incident Management  
- Potential Difficulties | Criteria for assurance for the different process domains are grouped into 4 phases. These are developed on the basis of “mirroring the rise of human civilization from primitive cultures to complex societies”  
I. Hunter-Gatherer  
II. Feudal  
III. Renaissance  
IV. Industrial  
Each of the above phases have brief statements, which describe the typical maturity of the enterprise security found at that level. The framework does not describe any ‘evidence’ requirements to substantiate the criteria at each level. | NO pre-defined metrics are described by the model, applicable across all process domains. Two of the process domains focus on security budget and budget spending, which tracks the costs and the allocations of financial resources by the organisation. Emphasis on measurement is also briefly mentioned at phase IV (Industrial) for the Business Perception process domain e.g. “Transaction security measured in real-time” |
Information Management Maturity Model (KPMG)  
*Note: The model is primarily about Information Management. For this discussion, only the related infosec domains are considered.*

The 9 process domains directly applicable to IT Security (out of 30) are identified below:  
- Principles, Policies & Standards  
- Roles and Responsibilities  
- User Awareness  
- User Training & User Support  
- Information Quality  
- Security  
- Risk Management  
- Business Continuity  
- Compliance

An incremental maturity model (5 levels) describes the criteria for each of the domains to be achieved to reach that level. "Each maturity level description is homogenous and does not represent more than one level of maturity."  
I. Non-existent/ Undeveloped  
II. Early stages of development  
III. Good Information Management Practices  
IV. Advanced Practices  
V. Industry Best Practices

The framework does not describe any confirmatory testing requirements to indicate that the organisation is on the correct path.

FITSAF (US Federal IT Security Assessment Framework: NIST SP 800-26, NIST SP 800-51)  

The criteria for assessment is grouped into 3 major control areas (i.e.) management controls (ii.) operational controls (iii.) technical controls. Within these control areas there are 17 individual and responsibilities issues ranging from Risk Management to Personnel Security to Audit trails.

This comprehensive framework while primarily aimed at government agencies (US) is applicable to other private organisations. For each criteria, the relevant reference to the source is provided (e.g. Act or other NIST guideline).

The framework advocates an incremental phased approach to check the effectiveness of the progress of the needed security controls. The 5 levels are:  
I. Control objective documented in a security policy  
II. Security controls documented as procedures  
III. Procedures have been implemented  
IV. Procedures and security controls are tested and reviewed  
V. Procedures and security controls are fully integrated into a comprehensive program.

For each claim (answer) to a question, there is a requirement for evidence in the form of references, which need to be detailed out in the Comments field. Additionally, the questionnaire contains a field that can be checked when a risk-based decision has been made to either reduce or enhance a security control.

NO metrics are defined to substantiate the maturity level assessment.


(www.sse-cmm.org)

The model describes a security engineering maturity model similar to the Capability Maturity Models developed by the Software Engineering Institute (SEI). The model describes 11 process areas directly related to the security engineering discipline. These are grouped into 3 major areas – Risk, Engineering and Assurance. They are:  
PA01 Administer Security Controls (E)  
PA02 Assess Impact (R)  
PA03 Assess Security Risk (R)  
PA04 Assess Threat (R)  
PA05 Assess Vulnerability (R)  
PA06 Build Assurance Argument (A)  
PA07 Coordinate Security (E)  
PA08 Monitor Security Posture (E)  
PA09 Provide Security Input (E)  
PA10 Specify Security Needs (E)  
PA11 Verify and Validate Security (A)

The aim of the model is to focus on the security engineering process as compared to suggesting a particular set of practices and security related controls.

The framework provides for assurance through the direct requirements of two process areas viz. PA-6 and PA-11. These process areas focus on defining the security objectives, evidence requirements and providing the argument that the security needs are satisfied.

The second source of assurance is the improvement model consisting of the different capability levels for the organisation to achieve. These are:  
Level 1: Performed Informally  
Level 2: Planned & Tracked  
Level 3: Well Defined  
Level 4: Quantitatively Controlled  
Level 5: Continuously Improving Quantitatively Controlled

Finally, the model is supplemented through an ‘Appraisal model’, which is a guideline explaining how to collect ‘evidence’ through a systematic approach to audit the security function of an organisation using the SSE-CMM model.

Metrics are defined by the set of metrics, which concentrate mainly on the comparison of control procedures and how well it is implemented and performing – the framework provides for organisations to quickly understand where their current status and where they need to improve.

The framework further stresses on the importance of metrics and rigorous testing in the latter levels.

Further guidance on defining the metrics, its use and application to the framework have been discussed exhaustively in the latest NIST publication SP 800-51.

COBIT (Control Objectives for Information Technology, IT Governance Institute)  
The Framework consists of a set of 34 high-level Control Objectives, grouped into four domains: planning and organisation (PO), acquisition and

While these 34 control objectives cover the entire domain of IT, for the purpose of this comparison, the following control objectives directly related to IT Security are identified as follows:  
PO2 Define the Information Architecture  
PO4 Define the IT Organisation and Relationships  
PO6 Communicate Management Aims and Direction  
PO8 Ensure Compliance with External Requirements

COBIT is a comprehensive tool designed specifically for IT Governance that tells the management about the risks and benefits associated with information and related IT.

In addition, corresponding to each of the 34 high-level control objectives is an Audit Guideline to enable the review of IT processes against COBIT’s 318 recommended detailed control objectives to provide management

Along with Maturity models, the Management Guidelines describe performance indicators for each of processes in the form of Critical Success Factors, which define the most important management-oriented implementation guidelines to achieve control over and within its IT processes; Key Goal Indicators, which define measures that tell management—after the fact—whether an IT process has achieved its business
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>P09 Assess Risks</td>
</tr>
<tr>
<td>A12 Acquire and Maintain Application Software</td>
</tr>
<tr>
<td>A13 Acquire and Maintain Technology Infrastructure</td>
</tr>
<tr>
<td>A14 Develop and Maintain Procedures</td>
</tr>
<tr>
<td>D14 Ensure Continuous Service</td>
</tr>
<tr>
<td>D15 Ensure Systems Security</td>
</tr>
<tr>
<td>D17 Educate and Train Users</td>
</tr>
<tr>
<td>D10 Manage Problems and Incidents</td>
</tr>
<tr>
<td>D11 Manage Data</td>
</tr>
<tr>
<td>D12 Manage Facilities</td>
</tr>
<tr>
<td>D13 Manage Operations</td>
</tr>
<tr>
<td>M1 Monitor the Processes</td>
</tr>
<tr>
<td>M2 Assess Internal Control Adequacy</td>
</tr>
<tr>
<td>M3 Obtain Independent Assurance</td>
</tr>
<tr>
<td>assurance and/or advice for improvement.</td>
</tr>
<tr>
<td>Cobit’s maturity model framework is described in its Management Guidelines, which provide management direction for getting the enterprise’s information and related processes under control, for monitoring achievement of organisational goals, for monitoring performance within each IT process and for benchmarking organisational achievement. The incremental scale is defined as follows:</td>
</tr>
<tr>
<td>0 Non-Existent</td>
</tr>
<tr>
<td>1 Initial</td>
</tr>
<tr>
<td>2 Repeatable</td>
</tr>
<tr>
<td>3 Defined</td>
</tr>
<tr>
<td>4 Managed</td>
</tr>
<tr>
<td>5 Optimised</td>
</tr>
<tr>
<td>According to the COBIT guidelines ‘Maturity Models management can map where the organisation is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organisation wants to be.’</td>
</tr>
</tbody>
</table>

Requirements; and Key Performance Indicators, which are lead indicators that define measures of how well the IT process is performing in enabling the goal to be reached.

Apart from the Management Guidelines, which describe in detail the metrics relevant to the different IT processes, CobiT also provides a Implementation Tool Set which among others features consists of two fundamental and useful tools for getting management’s attention & raising management’s awareness:

- IT Governance Self-Assessment
- Management’s IT Concerns Diagnostic

These tools assist in analysing, understanding and communicating an organisation’s IT control environment and the relevant IT control issues. These tools help in capturing the management’s view of – the level of importance of the control/process area, performance level of the controls for the different processes and the risk rating of the different IT processes.