CMM – Cyber Maturity Model

The best method to become "Cyber Competitive."

Otto P. Schmidbauer, PhD, BSI certified ISO 27001 Lead Auditor

Introduction

This paper describes the CYBERFENSE risk assessment platform and its capability to guide a commercial company through actionable "next steps" that will improve the quality of their security controls and continually reduce risk. The methodology is based on a defined cyber "capability maturity model" (CMM) mapped to a globally accepted information security standard. In effect, CYBERFENSE defines and measures capabilities of individual security controls and in consequence, rates an organization's overall cyber maturity.

The CYBERFENSE Capability Maturity Model® (CMM) focuses on improving the effectiveness of operational, technical and administrative processes of an organization. Our Capability Maturity Model® leverages the Carnegie Melon CMMI SVC 1.3 approach to determine the quality of a commercial organization's "security posture."

The optimization of a company's security posture is achieved by the following critical steps:

1) Measure each of the organization's "information security controls" against a globally accepted standard (ISO27001).

2) Map the organization's overall performance against a CMM model that serves as a both a referential benchmark and a roadmap from which Return on Investment (ROI) is measured.

3) Generate "next steps" that will lead maturity to the next level.

The CYBERFENSE platform is designed to help the non-technical, small and medium size business owners become "cyber competitive."

- Displays visual, intuitive output accessible from any device.
- Offers easy to understand, step-by-step guidance.
- Translates into industry compliance (e.g. COBIT5, HIPAA, CSF, ISA, etc.)
- Models performance against industry peers.

CMM CAPABILITY MATURITY MODEL

CMM Definition

Capability Maturity Model® (CMM) focuses on improving the effectiveness of the process control within an organization. CMMs contain and model the essential elements of effective processes for one or more disciplines and describe an evolutionary improvement path from ad hoc, immature processes to disciplined, more mature processes. CMM capability and maturity levels have become a widely accepted standard in the manufacturing and process control domain.

CMM Mapping

CYBERFENSE is an innovative leader. Our approach assigns ISO27001 ISMS Security Control Objectives (defined in Annex A of ISO27001: 2013) to "CMMI-like" domains. Doing so, this enables an organization to determine and optimize its "security posture" by benchmarking the current state of security risks then proposes practical improvements (ISO27002 best practices) to achieve the next level of maturity. This is what it means to become "cyber competitive."

The optimization of security risks is achieved in the following way:

An organization's existing "information security controls" are assessed relative to ISO27001; the implementation of each control is evaluated according to the CMM model, by determining the quality (expressed in capability or maturity) of the "security posture". A high maturity level means a low risk, and can be interpreted that the security control objectives are met to a high degree.

CYBERFENSE proposes mitigation paths towards a more complete implementation. All recommendations align to ISO27002 *Code of Practice for Information Security Controls* and descriptive information lead to the next higher maturity level.

In analogy to the CMMI "process areas", CYBERFENSE has defined a total of 43 "risk assessment domains." These risk domains correspond to ISO 27001:2013 Annex A control objectives, but some ISO control domains have been split in several parts, to achieve a more detailed description of the risk. Each risk domain is assigned a maximal achievable CMMI "maturity level." Table 1 below shows the definition of the CYBERFENSE risk domains (R1-R10) with the corresponding ISO 27001:2013 Annex A controls, together with

the maximal achievable maturity levels, for the case that all controls for a certain domain are in place.

#	Risk Domain Description	Maturity Level	CNTRL 1	CNTRL 2	CNTRL 3	CNTRL 4	CNTRL 5
R01	Security governance / Policies	3	A.05.1.1	A.05.1.2			
R02	Organizational Security Framework	3	A.06.1.1	A.06.1.2	A.06.1.5		
R03	Regular update of security practices	3	A.06.1.3	A.06.1.4			
R04	Mobile devices and teleworking	3	A.06.2.1	A.06.2.2			
R05	Due diligence for new contracts	3	A.07.1.1	A.07.1.2			
R06	Execution of work contracts	3	A.07.2.1	A.07.2.2	A.07.2.3		
R07	Termination of work contracts	2	A.07.3.1				
R08	Management of organizational assets	3	A.08.1.1	A.08.1.2	A.08.1.3	A.08.1.4	
R09	Classification of Information	3	A.08.2.1	A.08.2.2	A.08.2.3		
R10	Disposal of media	3	A.08.3.1	A.08.3.2	A.08.3.3		

Table 1: Subset of 10 of 43 Risk Domains.

In our system, each control (e.g., A.8.1.1, A.8.1.2) is described by a capability/maturity level scale, which is defined as follows:

- 0 - Ad hoc (initial)
  Some cyber initiatives are taken, but there is minimal measurement, methodology and strategy, action is reactive.
- 1 - Learning (managed)
  The Company begins to structure and organize around a coherent cyber strategy, but sometimes still reactive.
- 2 - Under control (defined)
  The Company manages processes and proactively implements robust controls.
- 3 - Predictive (optimized)
  The Company maintains a strategic advantage over competitors with controlled, measured and continuously reviewed cyber security processes.

Based on the risk assessment, the CYBERFENSE CMM analysis algorithm assigns a final maturity score to each risk domain based on a context-sensitive evaluation of the capability scores of individual controls.

CMMI output examples

Table 2 below shows an output example displaying risk domains (R01 – R06) labeled with the assessed maturity levels (see descriptions above). Based on a preprocessor, risk domains can be excluded as non-relevant depending on industry type or size of company.

Table 3 displays and example of a descriptive analysis of risk domain R02 – Organizational Security Framework currently at maturity level "1"; in order to reach the next level "2", a verbal description of maturity level "2" (Under control) is provided and recommendations for controls to be improved are provided (for different security standards, such as ISO27001, NIST Cybersecurity Framework (CSF), etc.).

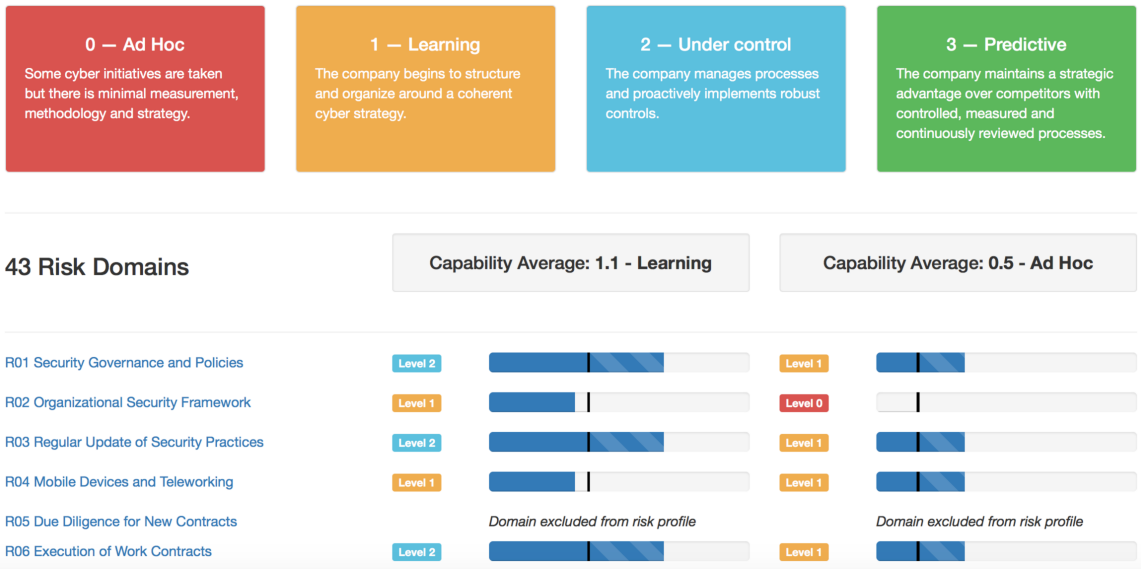

Table 2: Maturity level output overview for first 6 risk domains

A real-world example, is a business that wants to formalize their approach to cyber risk management and take the first steps towards becoming "cyber competitive." The CYBERFENSE risk engine identifies security and compliance gaps then generates a prioritized road map and recommends 'next steps.' The upfront value displaces the once costly and time-consuming assessment activities of the past and thus, unlocks significant savings that can be better spent on actual protections.

Another example is a large supply chain. It wants an idea of the inherited risk from sharing core information systems with thousands of 3rd party vendors. CYBERFENSE can be pushed down to each of its vendors for free as a value add. The supply chain owner now has continual oversight and can leverage risk management as a metric for contract performance.

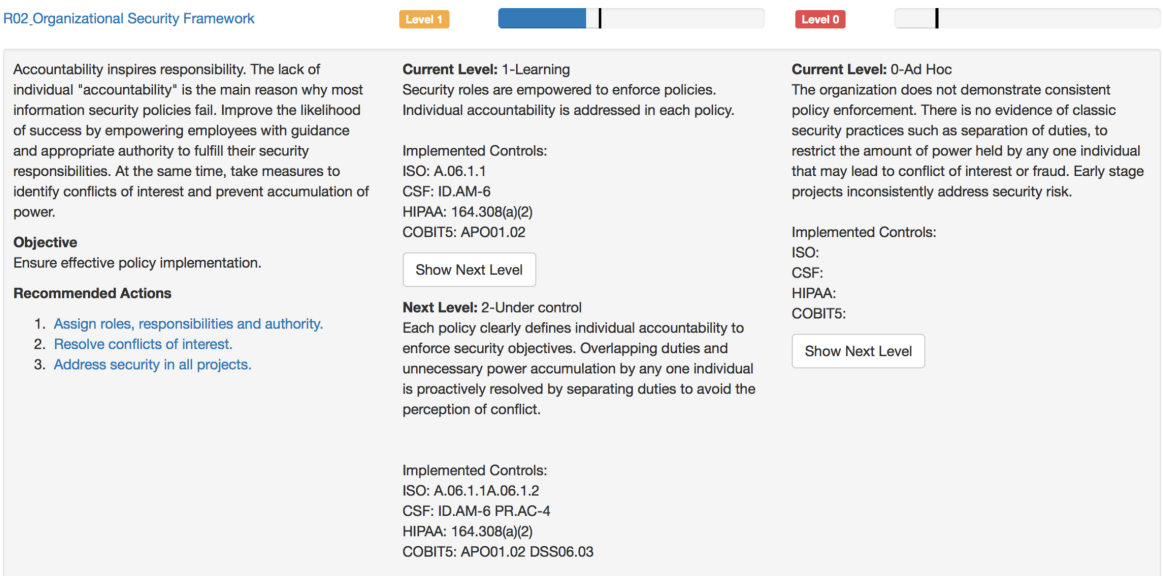

Table 3: Maturity level output for R02 with descriptive analysis with improvement recommendations (based on ISO27002) to achieve the next level.

Summary

In this paper, we have described in detail the CYBERFENSE CMM model. It provides actionable "next steps" to improve the quality of security controls and reduce overall risk.

CYBERFENSE takes a risk-based approach. The CMM process adapts to an organization's changing business objectives and future security challenges.

- Adaptive: Risk framework addresses different needs for cyber security depending on industries/businesses.
- Comprehensive: Evaluates all areas (organization, operations, processes) with a repeatable and standardized assessment method.
- Effective: Prioritizes and aligns risks according to business objectives and as such, focuses on what matters (top risks, top assets).

Otto Schmidbauer, PhD.

Dr. Schmidbauer, co-founder of CYBERFENSE, is responsible for statistical risk and data management. He started his professional career at Siemens Research Labs in Munich in the mid 80's at the early stages of artificial intelligence. His research focus was in Machine Learning and Statistical Pattern Recognition for Speech Understanding systems. As a guest researcher at the Computer Science Institute at Carnegie Mellon University, Pittsburgh, he gained deep experience in Neural Networks.

During his professional career, Dr. Otto Schmidbauer has developed a broad background in Man-Machine and Machine-to-Machine communication in different industries such as Telecom, Industry 4.0, Risk Analysis and Cyber Security. He held several senior positions in Consulting, Business Development and Project Management for innovative solutions.
Dr. Schmidbauer holds a Diploma degree and a Ph.D. in EE/Telecommunications from the Technical University Munich. Dr. Schmidbauer is a certified ISO/IEC 27001 Lead Auditor.