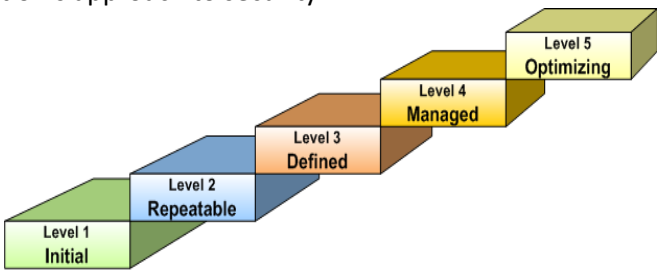
Enterprise Security Maturity

Combining the Capability Maturity Model (CMM) with Information Security Standards to Mitigate Information Security Risks

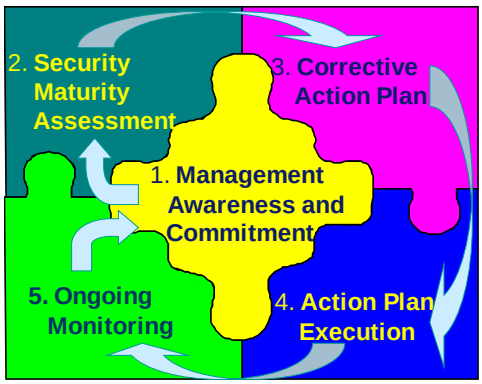
Time and again, speakers at information security conferences have warned audiences about the risks posed to their organizations by internal and external attacks. Yet in most cases, the talks highlight all the dangers without proposing a clear course of action. Security standards, such as ISO 27001/27002, are useful as a taxonomy of information security risks, but not as a methodology to address and mitigate them.

cébé IT & Knowledge Management offers a powerful and patented[1] combination:

- The Capability Maturity Model (CMM), originally invented at the Software Engineering Institute (SEI) to address software engineering quality, provides the process-oriented framework to assess the organization's approach to security.



- The ISO standards provide a recognized list of security aspects, which the CMM helps classify in a more actionable way. Some items in the standard, located in different sections, pertain to the same aspect of security, but represent different levels of maturity (e.g., the existence of a security policy vs. the fact that employees are aware of it and receive training about it). Our methodology uses the CMM to regroup these items logically, making it possible to assess the level of maturity without having to address the same topic repeatedly during an assessment.
- The general approach to quality improvement, based on W. Edwards Deming's original total quality management work ("plan, do, check, act"), provides the overall "virtuous circle" approach:



The methodology includes pragmatic advice to perform an assessment, asking questions from a representative audience without leading them to "politically correct" answers.

The deliverables of a Security Maturity Assessment come in two forms:

- A "security maturity profile" of the organization, of which the figure below is just one section.

ISO Category	ISO Section Number and Name		Level L1	L2	L3	L4	L5
Asset Classification and Control	I.1	Coverage					
	I.2, I.4	Classification					
	I.3	Ease of Alteration					
	I.5	Handling Procedures					
Security Policy	II.2, VII.5	Coverage and Review					
	II.1, VI.5	Availability and Training					
	II.3	Review of Process					

Assessed Maturity | Gap | Goal | Goal Exceeded

- A plan of action to improve the weaker areas, derived from the detailed "assessment matrix" that is part of the method.

[1] "Security Maturity Assessment" US Patent No. 7290275, issued in 2007. Inventors: Claude Baudoin and Colin Elliott.

cébé IT & Knowledge Management