



Security Maturity: a matter of effective integration

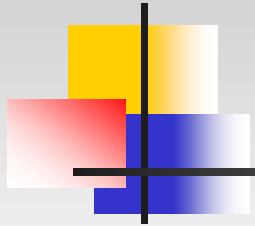
Bar Biszick-Lockwood, cisa, cissp, csqa
IT Quality and Security Assurance
www.qualityit.net
<mailto:barbis@qualityit.net>





Agenda

- Problem Definition
- Model characteristics
- Current candidates
- Security maturity defined
- Conclusions
- Contact info



Why is this so hard?

*Security requires a
fundamental shift in perspective by the
entire organization.*



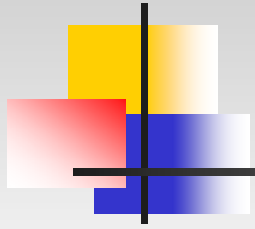
What is needed

Practical guidance for coordinating security efforts and incrementally improving it across the organization



Optimal Security Maturity Model Characteristics

1. Tells how, as well as what to do
2. Allows you to start from where you are
3. Incrementally improves all security areas concurrently
4. Coordinates security efforts across groups



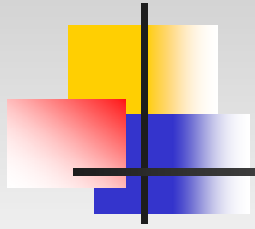
Characteristic 1:

Tells how, as well as what to do

Types of Standards

- Conceptual
- Referential
- ■ Implementation

There are several types of standards. Most are conceptual. What is needed are implementation standard that guides you in "how" to apply the principles embodied in these security standards



Characteristic 2:

Allows you to start from where you are

Unless you're starting from scratch, the approach most valuable to you are those standards that provide a roadmap for security improvement, not those that define ideal security, which is probably not achievable.

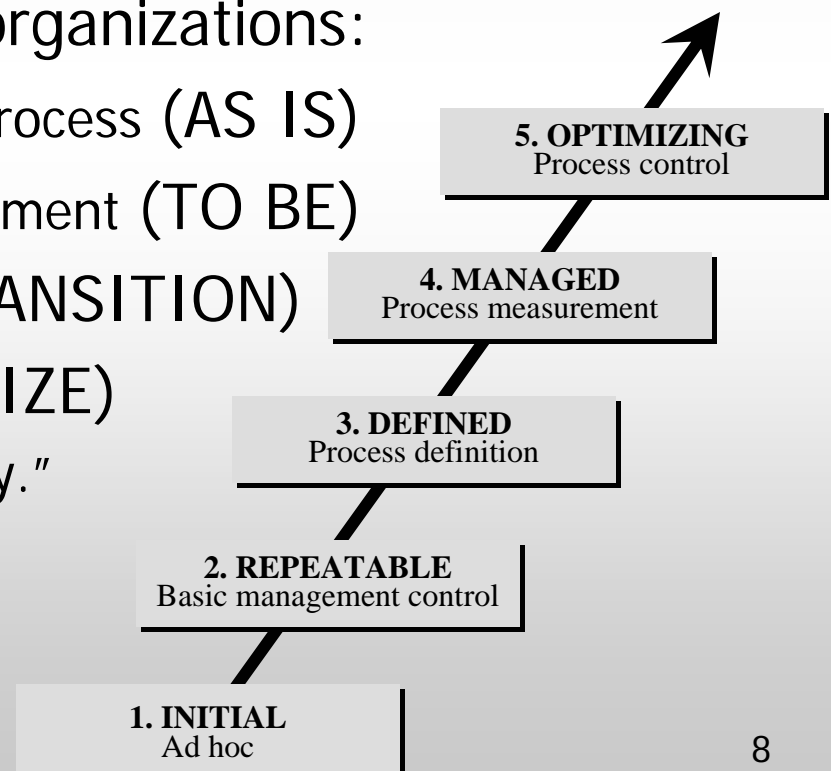


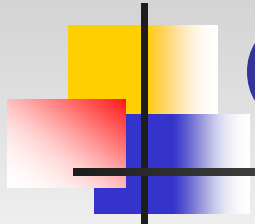
Characteristic 3: Incrementally improves all security areas

For instance: CMM for Quality Improvement
Defines Capability Maturity Levels

“A conceptual framework to help organizations:

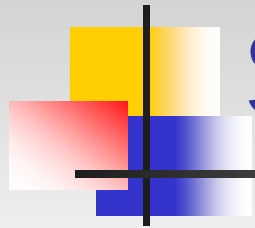
- characterize the maturity of their process (AS IS)
- Establish goals for process improvement (TO BE)
- Set priorities for getting there (TRANSITION)
- Manage & sustain change (STABLIZE)
- And introduce change incrementally.”





Controls Frameworks

- **Control Frameworks**
 - **ISO9001:2000**
 - **CobiT**
 - **Six Sigma**
 - **CMMI**
 - **ITIL**
 - **Octave**
 - **COSO**



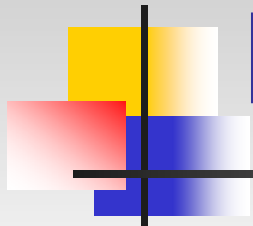
Security Guidance

- **ISO/IEC 17799**



Hybrids

- **SSE-CMM**
- **CobiT Security Baseline**
- **ITIL-COBRA**
- **(COSO)**



Key problem

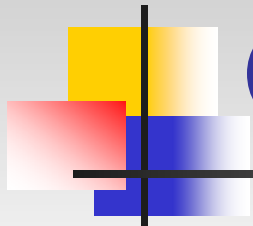


Security is a cross-disciplinary organizational risk problem.

There's a lack of coordination between security efforts across organizations

Characteristic 4: Coordinates security efforts across groups

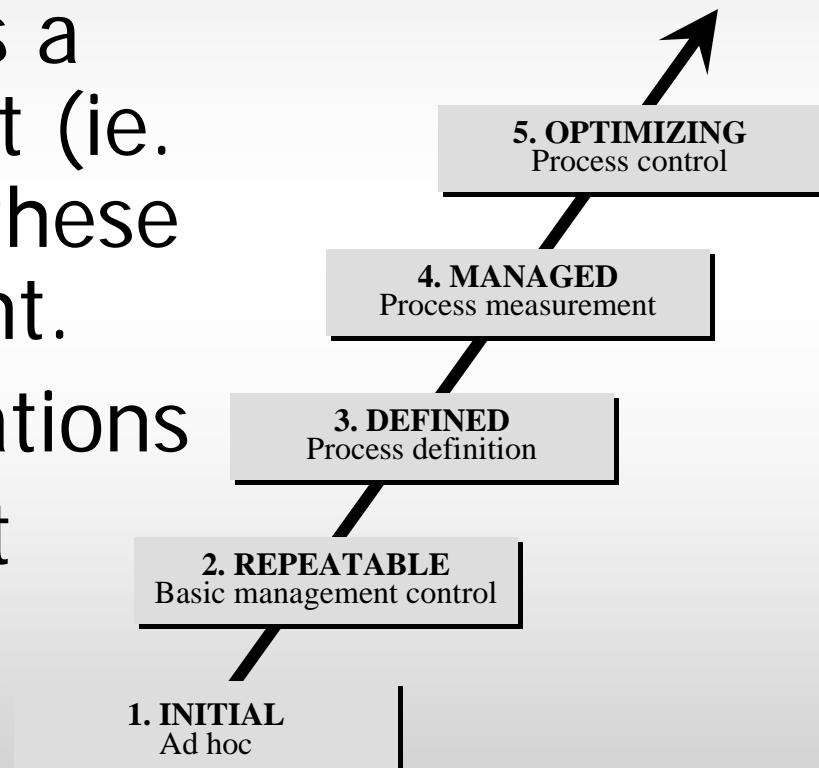




Capability Maturity Levels

If security is regarded as a separate controls effort (ie. implementing 17799) these levels might be relevant.

But for most implementations a separate control effort can be avoided.



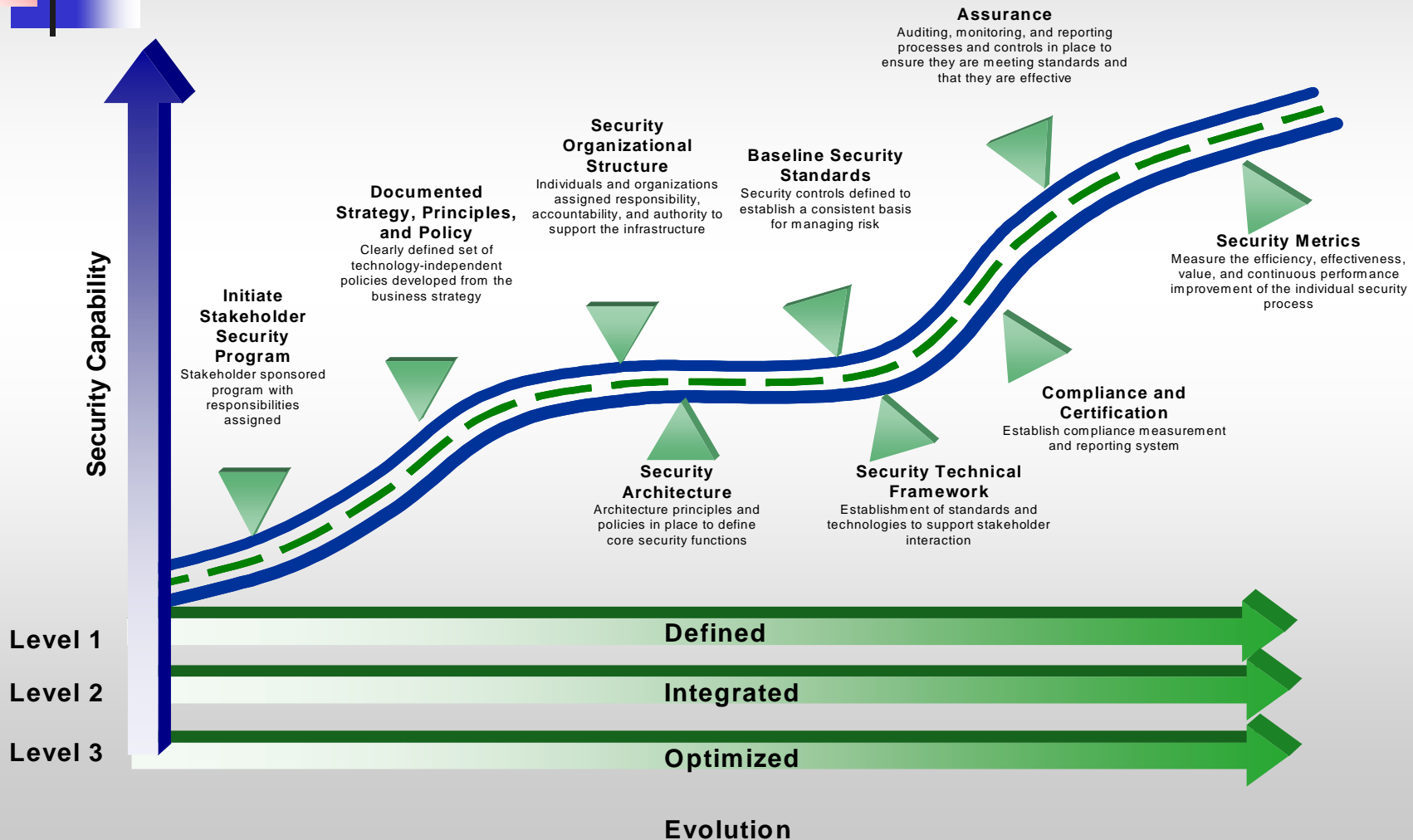


Why?

Phase based Capability maturity can be most efficiently applied when security is effectively integrated with other processes—not handled as a separate organizational process.

Therefore, a better measure of security maturity is the level of effective integration of security into existing organizational processes on which these frameworks depend.

Security Maturity Model (Three Levels)





Solution Approach

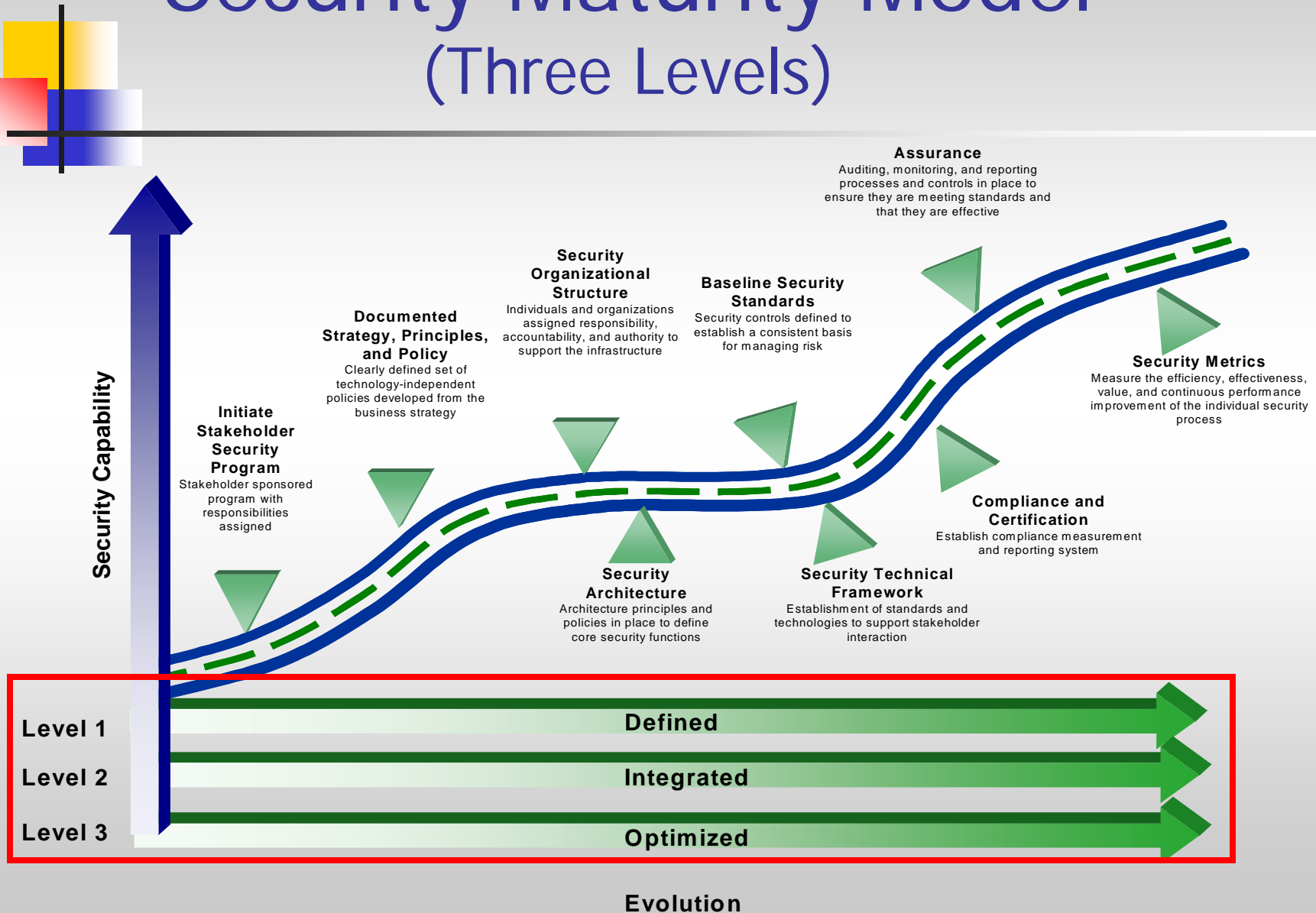
- Baseline current security posture
- Enhance current controls framework with security (or alternatively, adopt a hybrid common controls framework)
- Use common methods of risk analysis to prioritize security appropriately in the controls framework models.
- Focus energies on achieving the three organizational integration Security Maturity Levels (**Defined, Integrated, Optimized**)



Conclusions

- Dedicated Security maturity models are redundant. Current capability maturity models can be leveraged if security is fully integrated with organizational process, not dealt with as a separate problem domain.
- Security maturity should NOT be defined as the phase achievements of capability maturity models, but as the level of successful integration with other organizational processes.

Security Maturity Model (Three Levels)





Contact Info

- Bar Biszick, cisa, cissp, csqa
 - IT Quality and Security Assurance
 - 206-388-3333
 - <mailto:barbis@qualityit.net>
 - <http://www.qualityit.net/>

