

# Security Maturity Model

Presented by Patrick C Miller, CISSP SSCP IAM

ITEC – Portland, OR

December 11<sup>th</sup>, 2003



## **Information security**

is a dynamic, constantly evolving, living system. Breakwater keeps ahead of the curve and anticipates threats to provide clients with highly responsive protection.



# Presentation Overview

- **Breakwater Security Associates Profile**
- **What is the SMM and why do we need it?**
- **Benefits, Expected Results and Typical Applications of the SMM**
- **The SMM Summary Matrix**
- **Components of the SMM**
- **The Model in Action**
- **The Security Maturity Score and Additional Uses of the SMM**



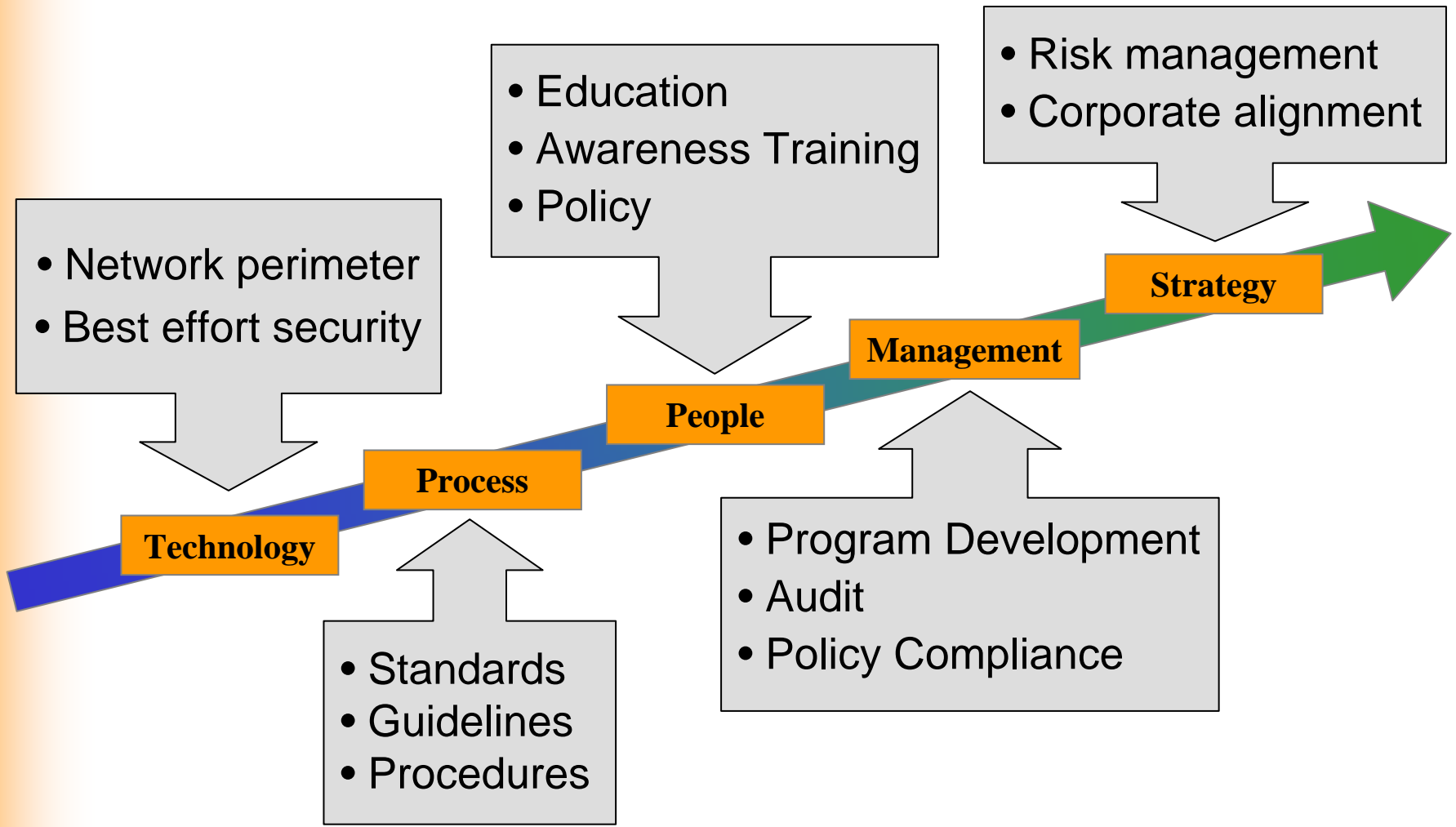
# Breakwater Security Associates

*Information Security and Risk Management Services Firm since 1996.*

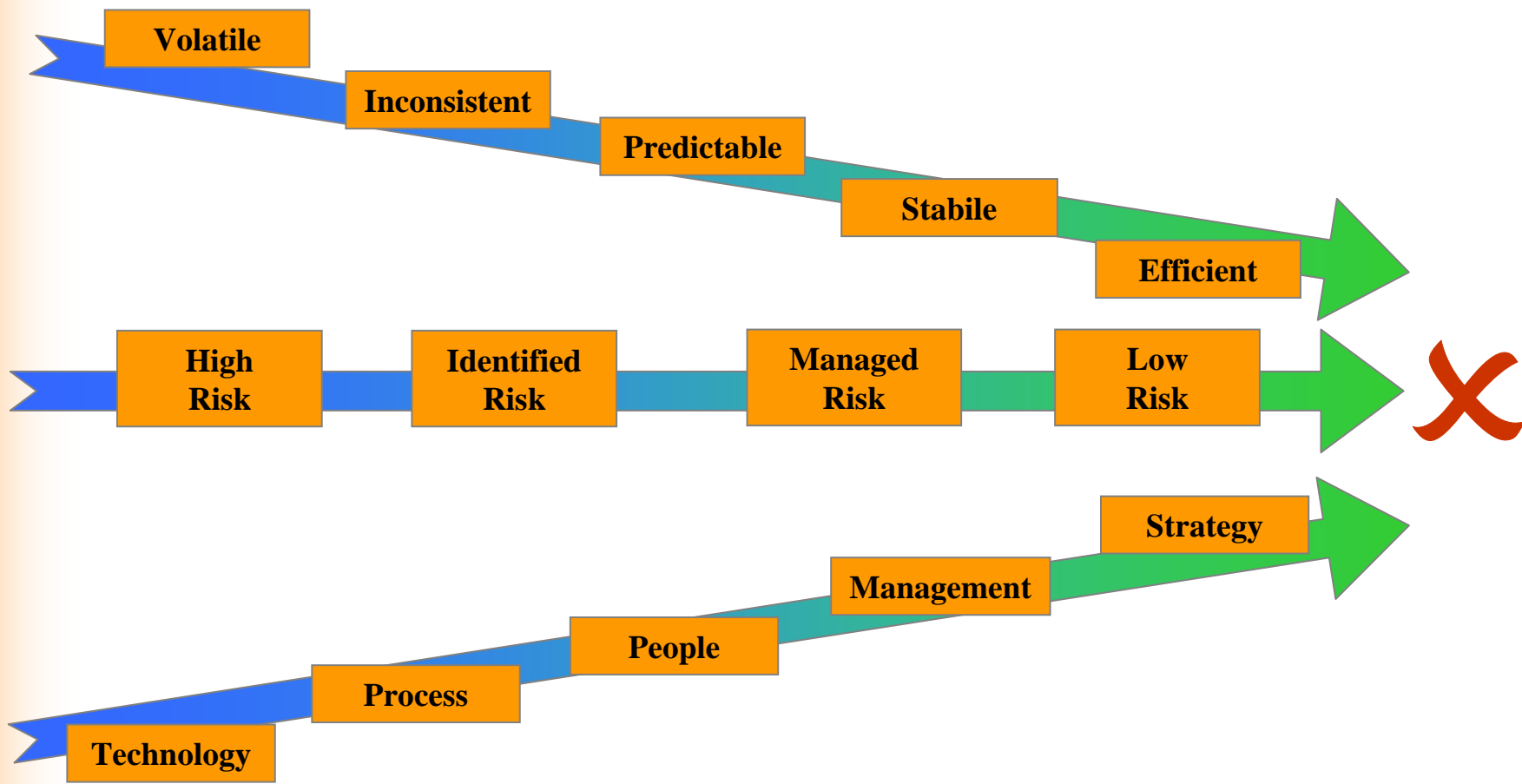
## **A few of the things we do well...**

- Security Program Development
  - Risk, Security and Vulnerability Assessments
  - Regulatory Compliance Gap Analysis
  - Policy Development and Auditing
  - Security Strategy
  
- Managed Security Services
  - Device Management
  - Event Correlation (Security Risk Management)
  - Monitoring

# Evolution of Security



# Evolution of Security





# What Is the SMM?

- The Security Maturity Model describes the essential characteristics of an organization's security process that must exist to ensure adequate and appropriate security.
- The model is a standard metric for security practices covering the following:
  - ✓ The entire life cycle, including development, operation, maintenance, and decommissioning activities
  - ✓ The whole organization, including management, organizational, and engineering activities
  - ✓ Interactions with other organizations, including compliance, acquisition, system management, certification, accreditation, and evaluation



# What Is the SMM - *Really*?

The Security Maturity Model is a repeatable and scientific method for measuring the overall maturity of any security process, based on industry standards.



# Why Do We Need an SMM?

- Security has many generally accepted principles, but no comprehensive framework for evaluation of security practices
- Higher quality products can be produced cheaper by increasing the quality of the processes that produce them
- To advance security within an organization as a defined, mature and measurable discipline



# Common Myths

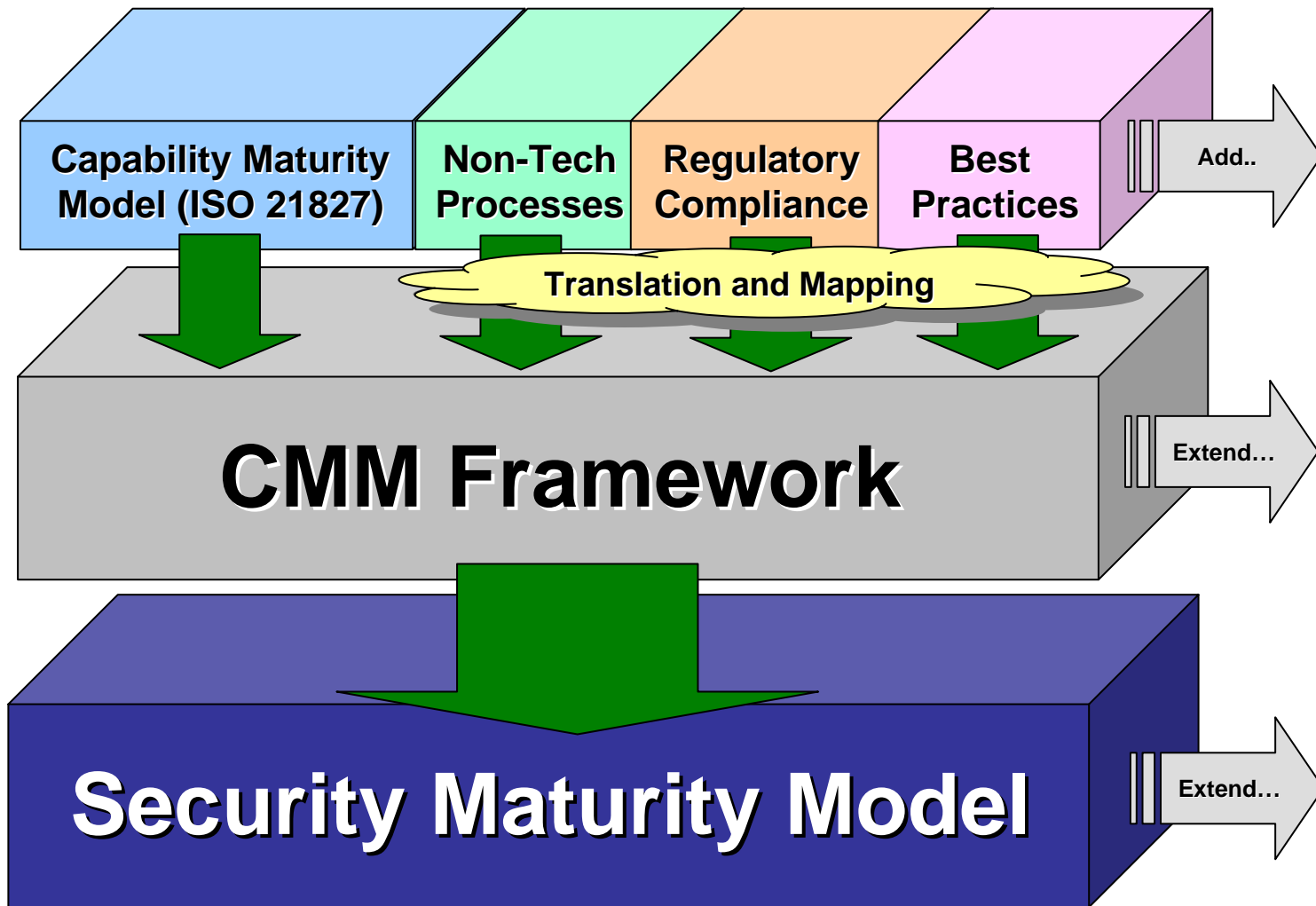
- Maturity Models define the process
  - CMMs provide guidance for organizations to define their processes and then improve the process over time – regardless of the particular process being performed
- Maturity Models are handbooks or training guides
  - CMMs are intended to guide organizations in improving their overall capability to perform a particular process – not to improve individual skills
- ISO 21827 is a replacement for product/service evaluation
  - Having a process under statistical control does not mean that defects are impossible – however defects can become more predictable
- Too much documentation is required
  - A number or type of documentation to be developed is not required
  - Depending upon the situation, a single document may suffice



# History of the SMM

- Started as CMM – Capability Maturity Model
  - NSA-sponsored effort in April 1993
  - Series of workshops and government/industry cooperation
  - *Core framework for SMM*
- SE-CMM and the SSE-CMM
  - SE-CMM (Systems Engineering Capability Maturity Model, 1995)
  - SSE-CMM (Systems Security Engineering Capability Maturity Model, 1997)
- ISO/IEC 21827
  - SSE-CMM officially became an ISO recognized standard in November, 2002
- SMMs - Security Maturity Models
  - ISO 21827 did not cover everything (i.e., regulatory), so more was needed
  - Mapping of current business processes to CMM framework
  - Mapping of current industry regulations to CMM framework
  - Mapping of industry-specific initiatives and programs to CMM framework
  - Application of SMM to vertical industries, organizations or organizational units over time for validation of model

# Security Maturity Model Stack





# Benefits of the SMM

**Continuity**

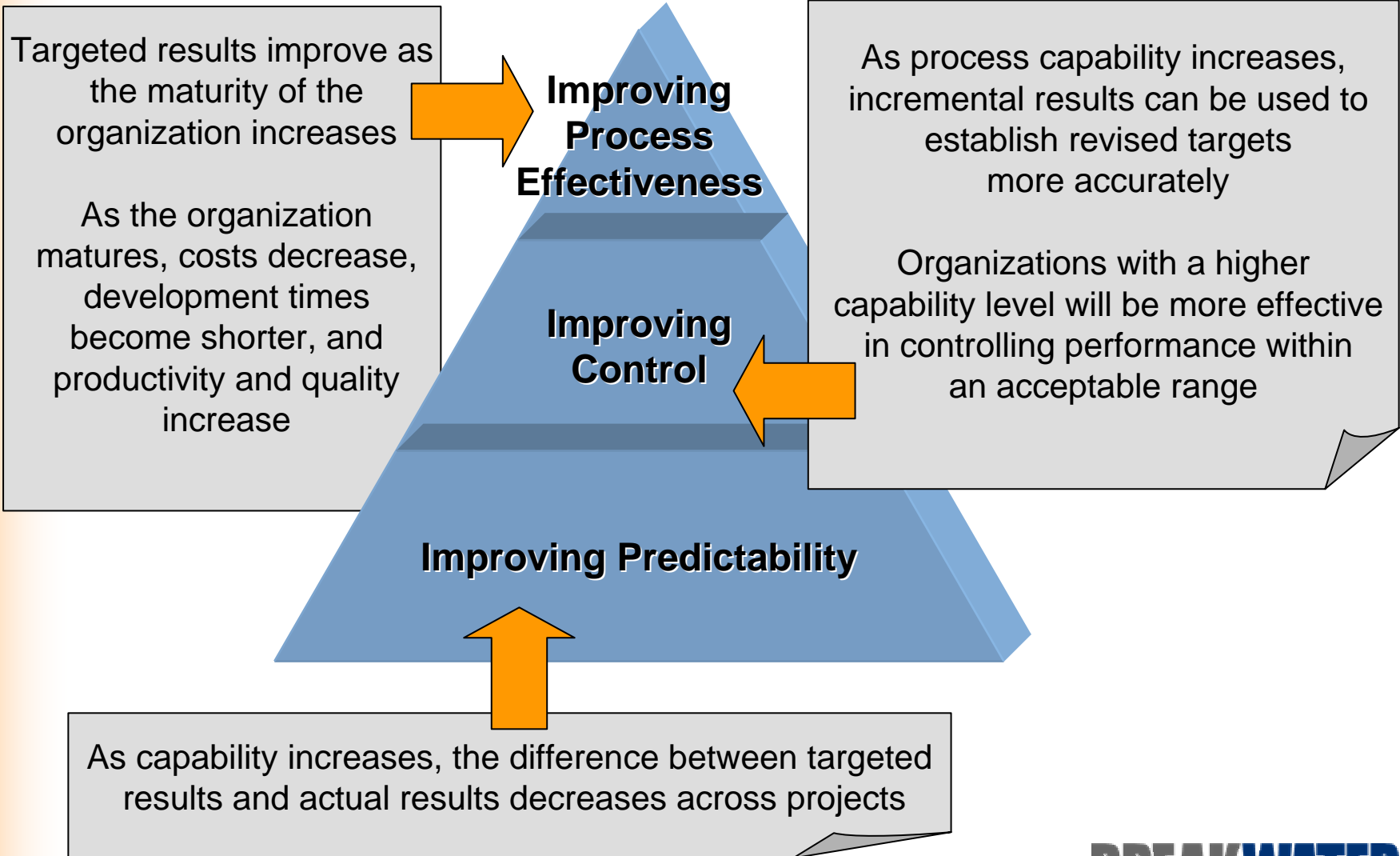
**Repeatability**

**Efficiency**

**Assurance**

- Savings with less rework from repeatable, predictable processes and practices
- Focus on measured organizational competency (maturity) and improvements
- Reusable process appraisal results, independent of system or product changes
- Confidence in security and its integration with other disciplines
- Capability-based confidence in evidence, reducing security evaluation workload

# Expected Results of the SMM





# Applying the SMM

## Typical Applications of the SMM:

- Tool for organizations to evaluate security practices and define improvements
- Basis for security evaluation to establish Security Assurance certifications or accreditations
- Standard mechanism for customers to evaluate a provider or business partner's security capability
- Make focused investments in security tools, training, process definition, management practices
- Establish trustworthiness in the maturity of the organization's security practices and processes

# The SMM Summary Matrix

## EXAMPLE: The Basic Model – Components of the SMM

Process Areas...

Capability Levels...

	Not Performed – 0	Performed Informally – 1	Planned and Tracked – 2	Well Defined – 3	Quantitatively Controlled – 4	Continuously Improving – 5
Security Management		1.0				
Human Resource Management		1.7				
Security Awareness Training			2.1			
Operational Security		1.9				
Contingency Planning			2.5			
Policy Review		1.3				
Facility Access Controls			2.9			

# The Process Areas...

## EXAMPLE: SMM Components – Process Areas

### Capability Levels...

	Not Performed – 0	Performed Informally – 1	Planned and Tracked – 2	Well Defined – 3	Quantitatively Controlled – 4	Continuously Improving – 5
Security Management		1.0				
Human Resource Management		1.7				
Security Awareness Training			2.1			
Operational Security		1.9				
Contingency Planning			2.5			
Policy Review		1.3				
Facility Access Controls			2.9			



# ...the Process Areas

## Process Areas (PA)


- Assemble related activities in one area for ease of use
- Relate to valuable security services
- Apply across the life cycle of the enterprise
- Can be implemented in multiple organization and product contexts
- Can be improved as a distinct process
- Include all Base Practices that are required to meet the goals of the process area



	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Process Area 1			2.0			
Process Area 2				3.5		
Process Area 3			2.9			

# The Capability Levels...

## EXAMPLE: SMM Components – Capability Levels



Not Performed – 0	Performed Informally – 1	Planned and Tracked – 2	Well Defined – 3	Quantitatively Controlled – 4	Continuously Improving – 5
-------------------	--------------------------	-------------------------	------------------	-------------------------------	----------------------------

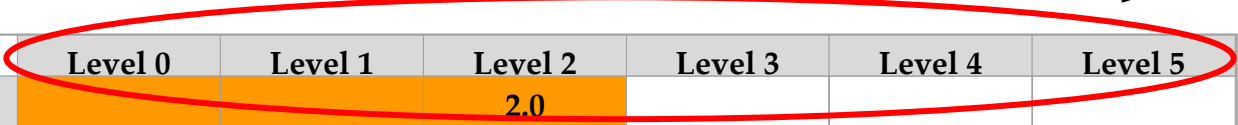

Process Areas...

Security Management	1.0				
Human Resource Management	1.7				
Security Awareness Training		2.1			
Operational Security	1.9				
Contingency Planning		2.5			
Policy Review	1.3				
Facility Access Controls		2.9			

# ...the Capability Levels

## Capability Levels:

- Level 0 – Not Performed
- Level 1 – Performed Informally
- Level 2 – Formally Documented
- Level 3 – Managed
- Level 4 – Quantitatively Controlled
- Level 5 – Strategic Planning



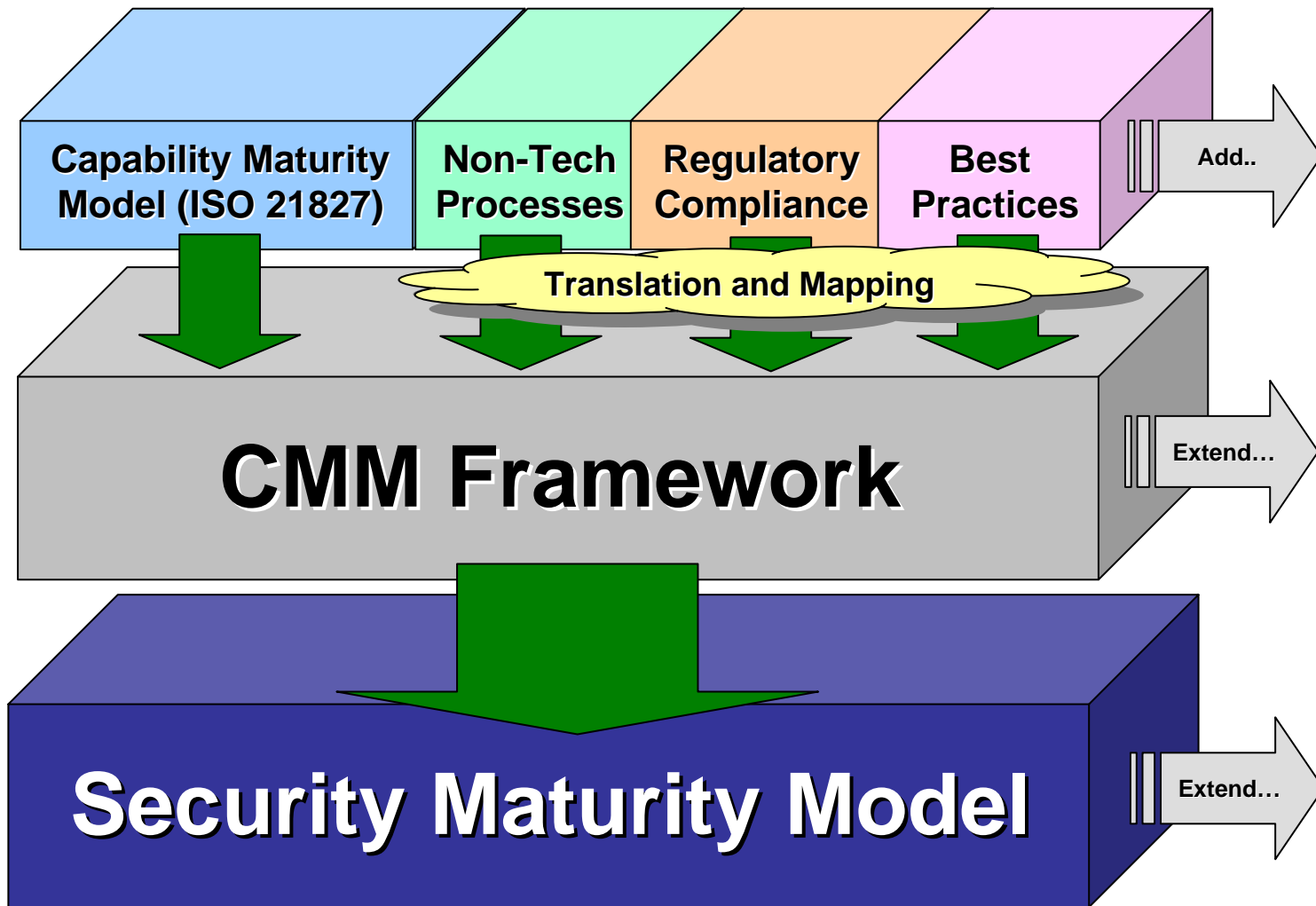
	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Process Area 1			2.0			
Process Area 2				3.5		
Process Area 3			2.9			



# Flexibility in the Model

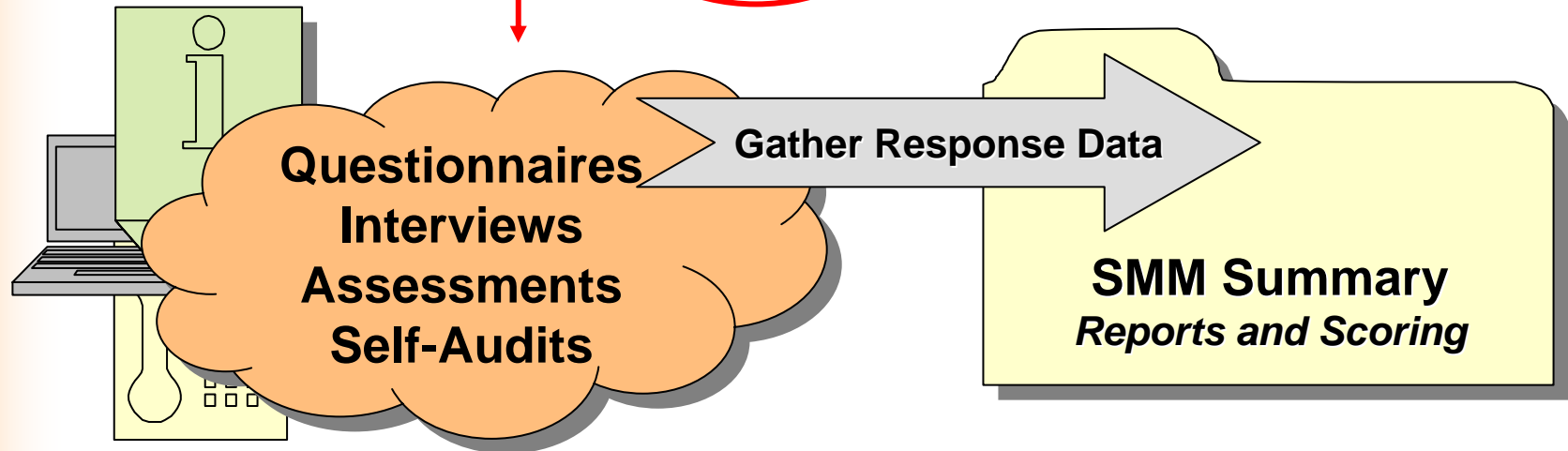
- **Process Areas are not finite**
  - Add organization-specific Base Practices
  - Add Regulatory Requirements
  - Add Industry Initiatives
  - Add Security Best Practices
- **Capability Levels are not finite**
  - Can be expanded to be more granular
- **Fully Customizable...**
- **CMM Framework is the core...**

# Security Maturity Model Stack



# The Model in Action...

ID	Question	0	1	2	3	4	5	Comment	Source
001	Question 001	X	X	X				Comment...	John Doe
002	Question 002	X	X	X	X			Comment...	Jane Doe
003	Question 003	X	X	X	X			Comment...	Jane Doe
004	Question 004	X	X	X				Comment...	John Doe
005	Question 005	X	X	X	X			Comment...	John Doe



# Security Maturity Score

## Sample

		Capability Levels					
		0 - Not Performed	1 - Performed Informally	2 - Planned & Tracked	3 - Well Defined	4 - Quantitatively Controlled	5 - Continuously Improving
Security Process Areas	Security Management		1.08				
	Human Resource Management		1.79				
	Security Awareness Training	0.75					
	Operational Security		1.00				
	Contingency Planning		1.33				
	Policy Review			2.00			
	Facility Access Controls		1.50				
	Device and Media Controls	0.75					
	Physical Security Incident Procedures		1.08				
	Access Controls			2.60			
	Authentication Controls			2.33			
	Account Management			2.50			
	Audit Controls		1.00				
	Host and Data Security		1.20				
	Transmission Security and Integrity		1.66				
	Electronic Security Incident Procedures		1.79				
	<b>Overall Security Maturity Score</b>	<b>1.52</b>					

Average of all  
Capability  
Levels from  
all Process  
Areas

# SMM Risk Comparison

Standard	Topic	Capability	Risk
Security Management Process		2.33	Med
	Security Sponsorship	2	Med
	Risk Assessment	3	Med
	Risk Management	2	Med
Human Resource Management		2.25	High
	Authorization	3	Low
	Hiring Procedures	3	Low
	Termination Procedures	2	Med
	Job Change Procedures	1	High

By integrating the SMM scores with other assessment data, the model becomes even more valuable

# SMM Benchmark Comparison

Organization	Process Area Group	Capability	Pass
<b>Business Unit 001</b>		<b>2.33</b>	<b>No</b>
	Administrative Security	2	N
	Physical Security	3	Y
	Technical Security	2	N
<b>Business Unit 002</b>		<b>3.00</b>	<b>Yes</b>
	Administrative Security	3	Y
	Physical Security	3	Y
	Technical Security	3	Y
<b>Business Unit 002</b>		<b>2.00</b>	<b>No</b>
	Administrative Security	1	N
	Physical Security	3	Y
	Technical Security	2	N



# Repetition is Good

1. Define and manage a comprehensive set of Process Areas
2. Perform initial SMM assessment
3. Validate and establish SMM baseline
4. Repeat the SMM assessments regularly
5. Generate a clear trend report of Security Maturity of the organization through time



# Questions?

**Patrick C Miller, CISSP SSCP IAM**

*Senior Security Consultant,  
Energy and Utility Practice Principal*  
pmiller@breakwatersecurity.com

503.517.3407 (desk)

503.312.0703 (mobile)