Fine Tuning IS Strategies Using Maturity Models

Goran Kovacevic, Chief Enterprise Architect, Visa.

Professional Strategies – S23

These are my thoughts/opinions, and do not represent the official position of any company, company's technology teams or anyone else in particular.

What is this session about?

- History of good and bad Strategies
- Applying the strategy building blocks to security
- Maturity models for information security
- Using maturity models for building strategies
- Questions?

HISTORY OF GOOD AND BAD STRATEGIES

The Battle of Trafalgar

Lord Nelson's strategy

- The British admiral's fleet was outnumbered at Trafalgar by an armada of French and Spanish ships.
- Lord Nelson strategy: Broke the British fleet into two columns and drove them at the Franco-Spanish fleet, hitting its line perpendicularly.

- Nelson's victory is a classic example of good strategy, which almost always looks this simple and obvious in retrospect.
- A good strategy does more than urge us forward toward a goal or vision; it honestly acknowledges the challenges we face and provides an approach to overcoming them.

Maginot Story

The French defense strategy after WW I

- A line of concrete fortification, obstacles, and weapons installations to prevent any further invasions from the east.

- The German army defeated the French army and conquered France in about six weeks.
- Bad strategy ignores the power of choice and focus, trying instead to accommodate a multitude of conflicting demands and interests.

Elements of good strategies

Strategy creation is a journey

Discover the crucial factors in a situation and design a way to coordinate and focus actions to deal with them.

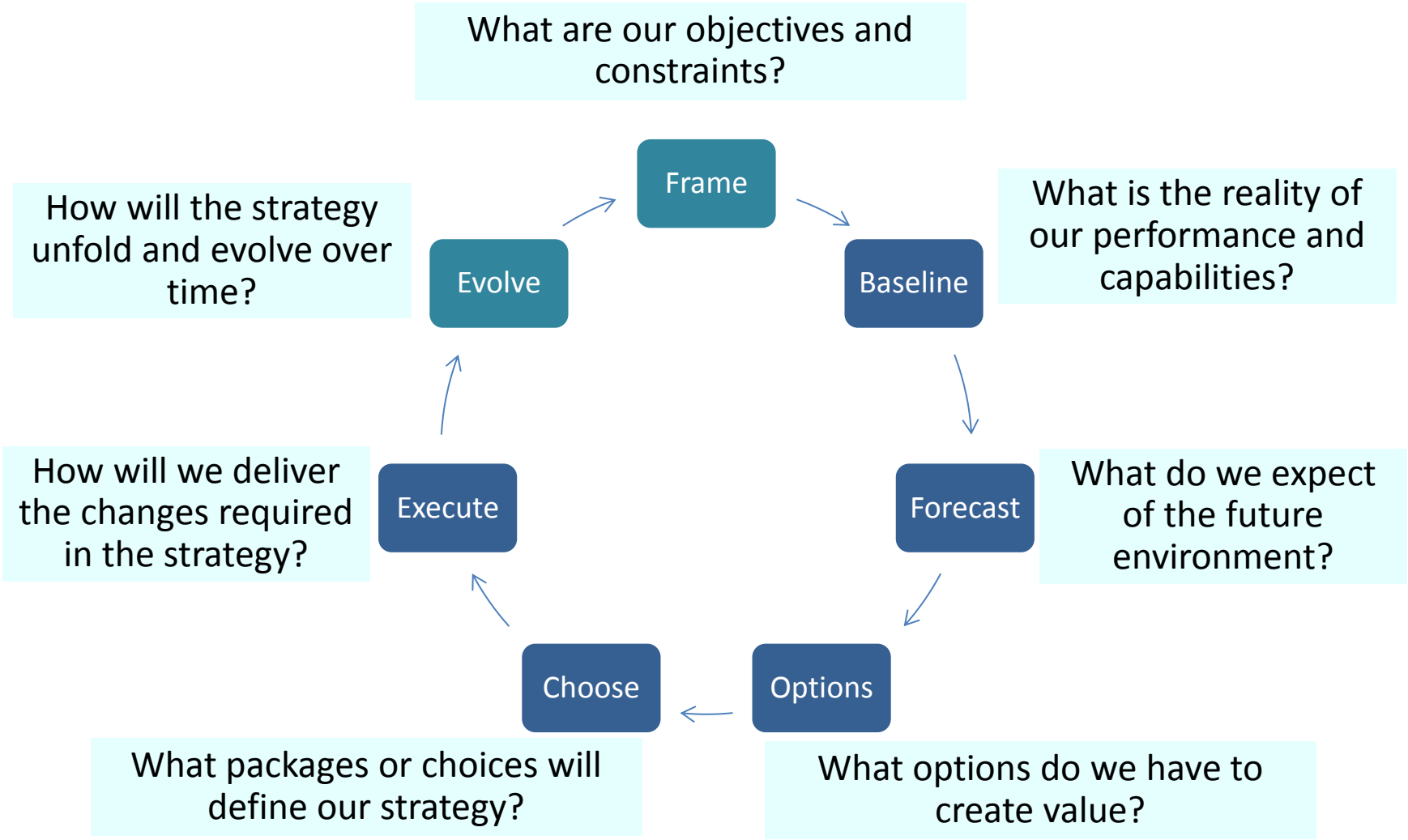
- A diagnosis: an explanation of the nature of the challenge.
- A guiding policy: an overall approach chosen to cope with or overcome the obstacles identified in the diagnosis.
- Simple objectives: Focusing energy and resources on pivotal objectives.
- Coherent actions: coordinated steps to support the accomplishment of the guiding policy.

At the end of the day, strategy is about the actions you take.

APPLYING THE STRATEGY BUILDING BLOCKS TO SECURITY

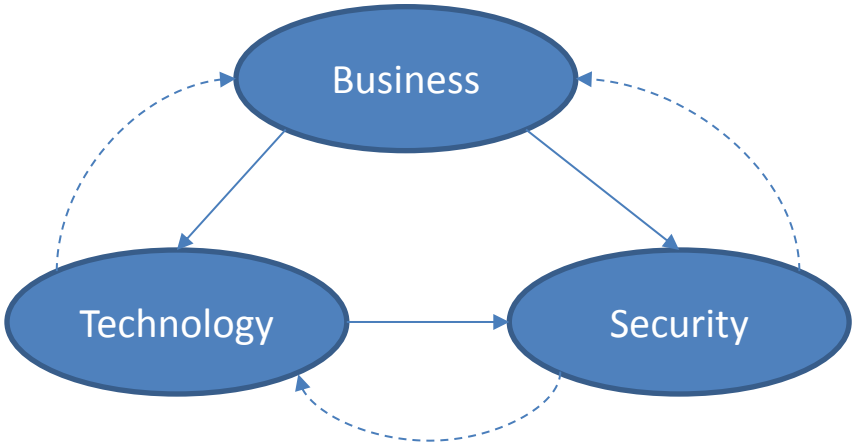
Strategy Core Building Blocks

What are questions to answer?



Business, Technology and Security Strategies

- Core building blocks approach is applicable to any strategy development
- Strategies are interconnected and dynamic
  - Change in business direction affects the technology and security strategies?
  - Changing risks and technologies may impact business strategies
  - Developing/updating a strategy is not an annual thing



- Security strategy needs business alignment
  - Results in optimized security efforts and investments.
  - Alignment of security service levels with the well-understood risk control needs of the business,
    - otherwise security efforts will always be either too expensive or inadequate.

Building Information Security Strategy

Frame	**What are our objectives and constraints?**	• Define decisions to be considered • Understand scope of potential solutions • Understand relevant resources and constraints • Identify key information assets • Identify high-risk areas • Identify SMEs and stakeholders • Clarify rules that will govern work
Baseline	**What is the reality of our performance and capabilities?**	• Understand sources of value at risk and past protection performance • Understand major drivers and changes in information security • Analyze available security capabilities
Forecast	**What do we expect of the future environment?**	• Identify emerging security trends and implications • Understand risk appetite and isolate critical uncertainties • Define desired security capabilities maturity • Develop realistic divergent scenarios
Options	**What options do we have to create value?**	• Establish and refine option set • Assess possible competitive responses • Evaluate options in given scenarios

Building Information Security Strategy

(Cont.)

Choose	**What packages of choices will define our strategy**	• Decide where and how to compete • Determine what, if any hedging is needed • Create coherent package (Strategy)
Execute	**How will we deliver the changes required in the strategy?**	• Develop action plan for selected options (Roadmap) • Determine investment priorities • Reallocate resources to finance plans • Determine how to communicate changes (Security Strategy and Roadmap) • Delegate key jobs to pivotal roles
Evolve	**How will the strategy unfold and evolve over time? How do we manage risks?**	• Execute agreed-upon action plans • Track ongoing progress • Determine revisions to be made • Determine when and how to compete

Structured Approach to Communicate Security Strategy

- Simple and easily understood format
- Clarify purpose, audience and objectives
- Provide Executive Summary
- Problem definition
  - Current state
  - Future state
  - A concise, structured and intuitively obvious description of the problem
- Strategy
  - The program of work that entails the strategy (proposed projects and resources)
  - Governance of the strategy execution
- Benefits
- Action Plan

MATURITY MODELS FOR INFORMATION SECURITY

Capability Maturity Models

- CMM: A framework using a set of structured levels that describe how well the practices of an organization can reliably and sustainably produce required outcomes.
- Capability Maturity Models (CMMs) help manage change
  - Describe the practices that organization must perform.
  - Measure current capabilities and improvements (assessment)
  - Help define short and long term target capabilities
  - Help manage the improvement efforts including cost and resources
  - Used for benchmarking – help understand how much is enough?
- CMMs have gained wide scale acceptance
  - Original capability maturity model - SW-CMM in the early 1990s
  - Increased interest in measuring maturity of IT, EA and IS

CMMs For Information Security (IS)

- The various practices are typically organized into five levels,
  - each level representing an increased ability to control and manage the environment.
  - Variations in naming's and definitions
- Many CMMs for IS (ISMMs) - but there is little consistency
  - Global IT Consulting Firms
  - Information Security Firms
  - Security Software Companies
  - Research Analysts
  - Federal Agencies
- Some recognized IS maturity models used in industry;
  - Forrester, Gartner, BSIMM, …

Why ISMMs?

- Enable CISOs and Security leaders to align IS with business and IT strategies
- Understand the full scope of their security responsibilities
- Identify where investments in people, process, and technology may or may not be consistent with what the business actually requires
- Prioritize the various initiatives, develop a coherent strategy, and articulate their value to the business.
- Monitor and report IS capabilities against changing business and IT practices
- Overall improvement of IS processes, communications, and business risk management

Forrester IS Maturity Model

- Allows S&R professionals to
  - identify the gaps in the security program and portfolio,
  - evaluate their maturity, and
  - better manage an overarching security strategy.
- The model consists of:
  - Four top-level domains
  - 25 functions, and 123 components
- Oversight role over functions in other domains

	ISO 27001/ 27002	COBIT 4.1	NIST 800-53	BITS	COSO	OCEG	Forrester ISMM
Oversight							
Strategy	●	●	●	●	●	●	●
Governance	◒	●	◒	●	●	●	●
Risk management	●	●	●	●	◒	●	●
Compliance management	●	●	●	●	●	●	●
Audit and assurance	●	◒	●	●	●	●	●
People							
Security services	◒	◒	◒	◒	◒	○	●
Communication	◒	●	◒	◒	◒	●	●
Security organization	●	●	◒	◒	◒	◒	●
Business relationship	●	●	○	●	●	●	●
Roles/responsibilities	◒	◒	◒	●	○	●	●
Process							
Identity and access management	◒	◒	◒	◒	○	◒	●
Threat and vulnerability management	◒	◒	◒	◒	○	◒	●
Investigations and records management	◒	◒	●	●	○	●	●
Incident management	◒	◒	◒	◒	●	◒	●
Sourcing and vendor management	●	●	●	●	●	◒	●
Information asset management	●	◒	●	●	◒	●	●
Application/systems development	◒	○	◒	○	○	○	●
Business continuity and disaster recovery	●	●	◒	●	◒	●	●
Technology							
Network	◒	●	◒	●	◒	○	●
Databases	○	◒	●	◒	○	○	●
Systems	○	◒	◒	●	○	◒	●
Endpoints	◒	○	◒	◒	○	○	●
Application infrastructure	◒	◒	●	○	○	○	●
Messaging and content	◒	◒	◒	○	○	○	●
Data	◒	◒	●	◒	○	◒	●

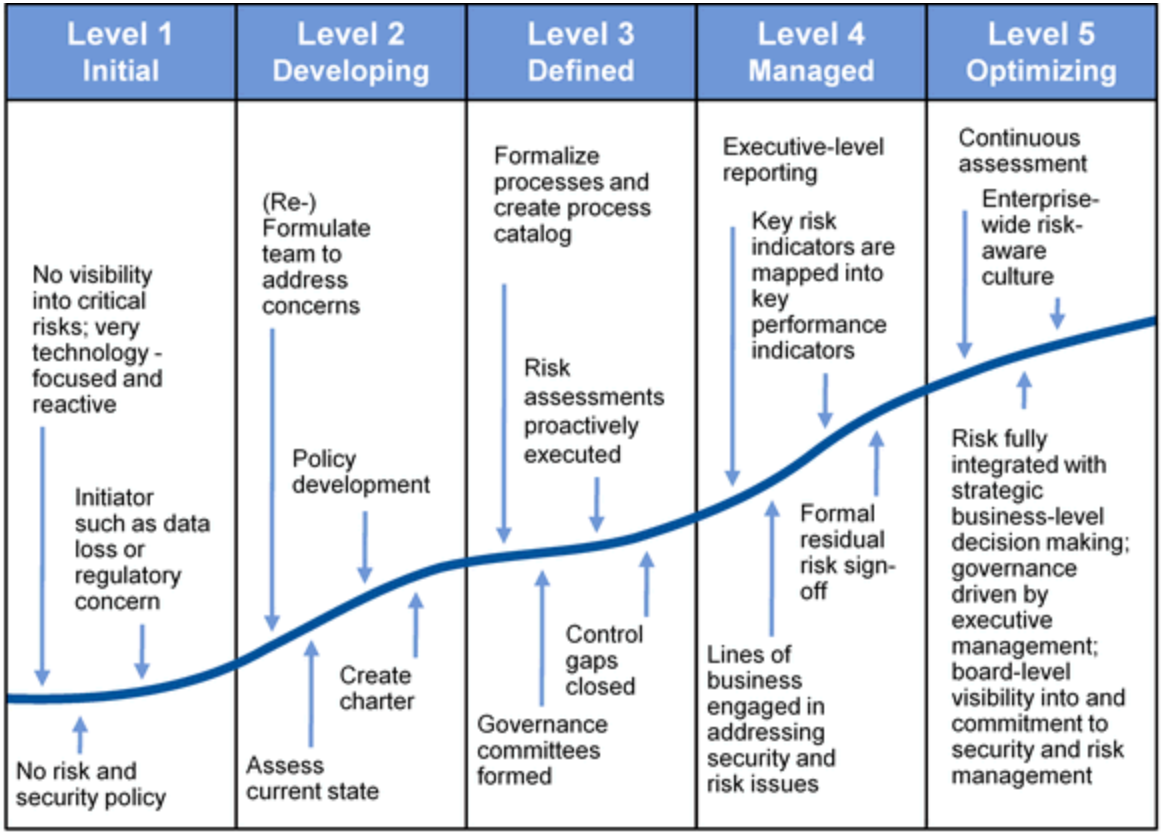
○ Doesn't cover ◒ Some coverage ● Full coverage

56671 Source: Forrester Research, Inc.

Gartner IS Maturity

- Six areas for security and risk management

- Business continuity management
- Compliance
- Identity and Access Management
- Information security management
- Privacy
- Risk management practices



Building Security In Maturity Model

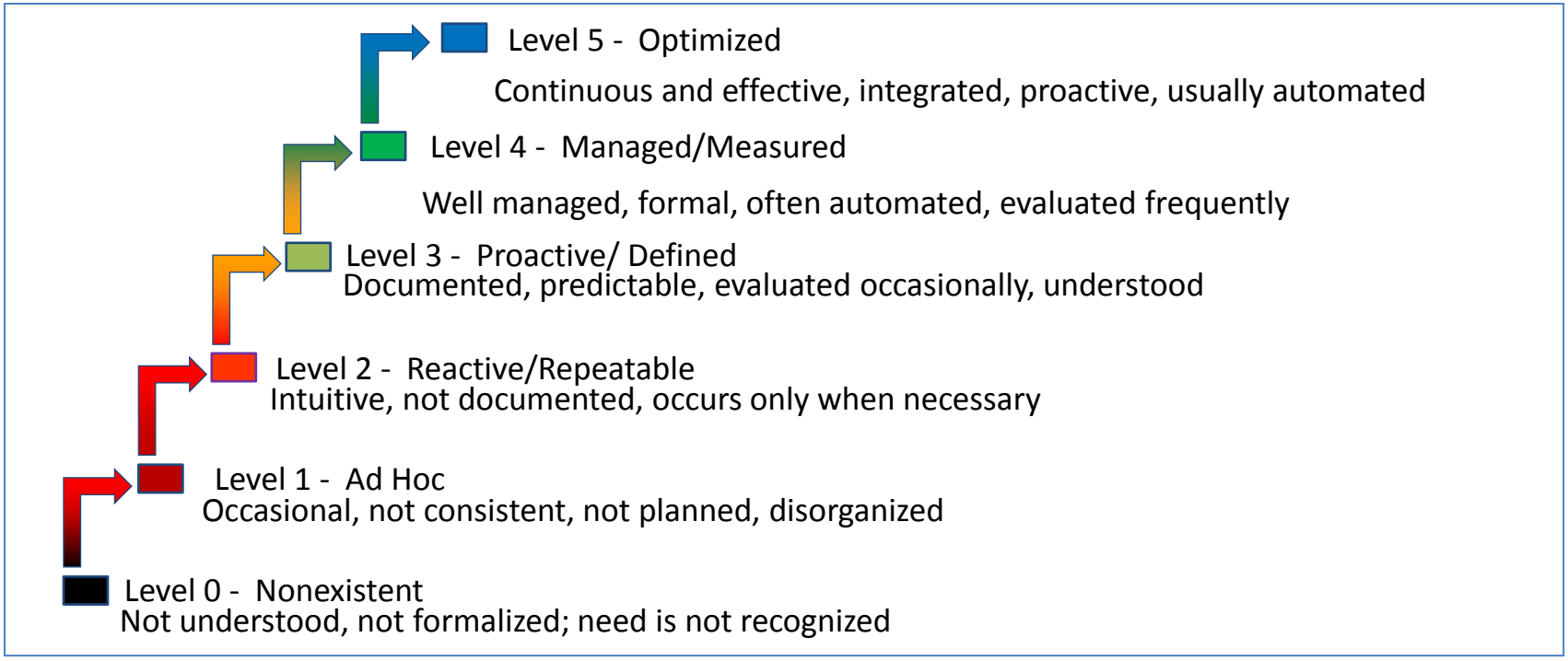
BSIMM (pronounced “bee simm”) by Cigital

- A study of real-world software security initiatives.
- Built entirely from observations made by studying sixty-seven real software security initiatives.
- The BSIMM does not tell you what you should do; instead, it tells you what everyone else is actually doing.

The Software Security Framework (SSF)			
Governance	**Intelligence**	**SSDL Touchpoints**	**Deployment**
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Manage-ment

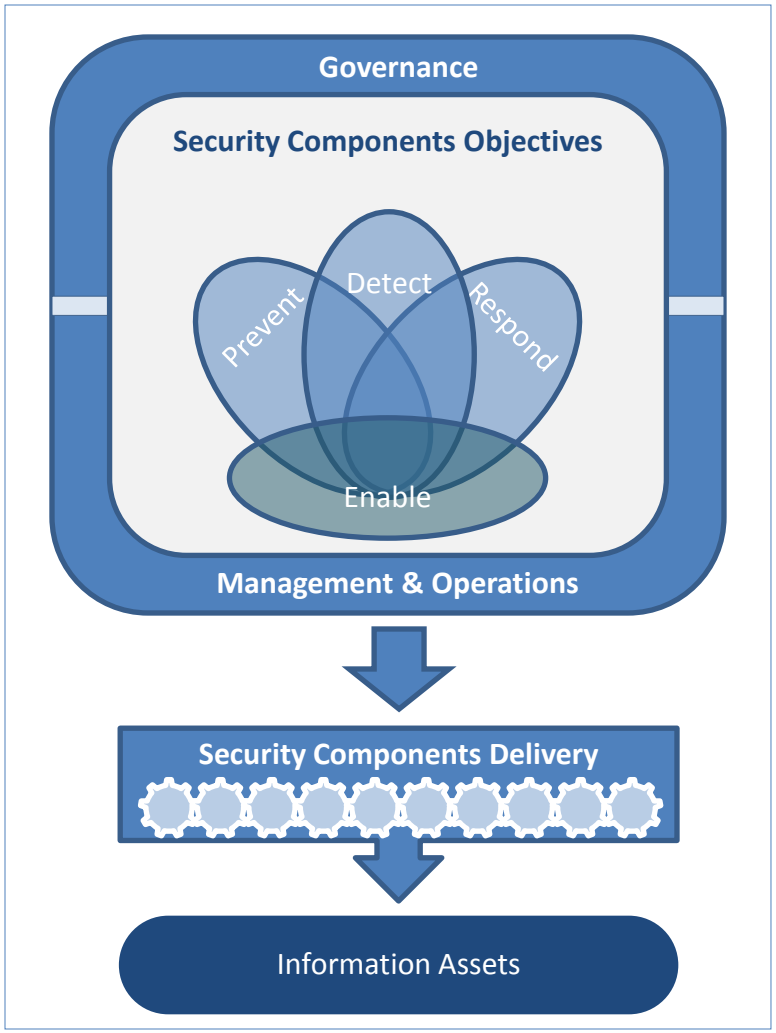
Integrated ISMM

- Leverages previously discussed models plus MORE
- Enables the creation/adjustment/continuous improvements of the IS Management Programs (ISMP)
- Ratings based on the COBIT maturity level definitions (0 – 5)



Approach to Building ISMM

- Leverages IS Management industry standards, frameworks and practices
- Information security capabilities are evaluated from Process, People and Technology perspectives
- Security capabilities are delivered through security components to business and technology platforms.



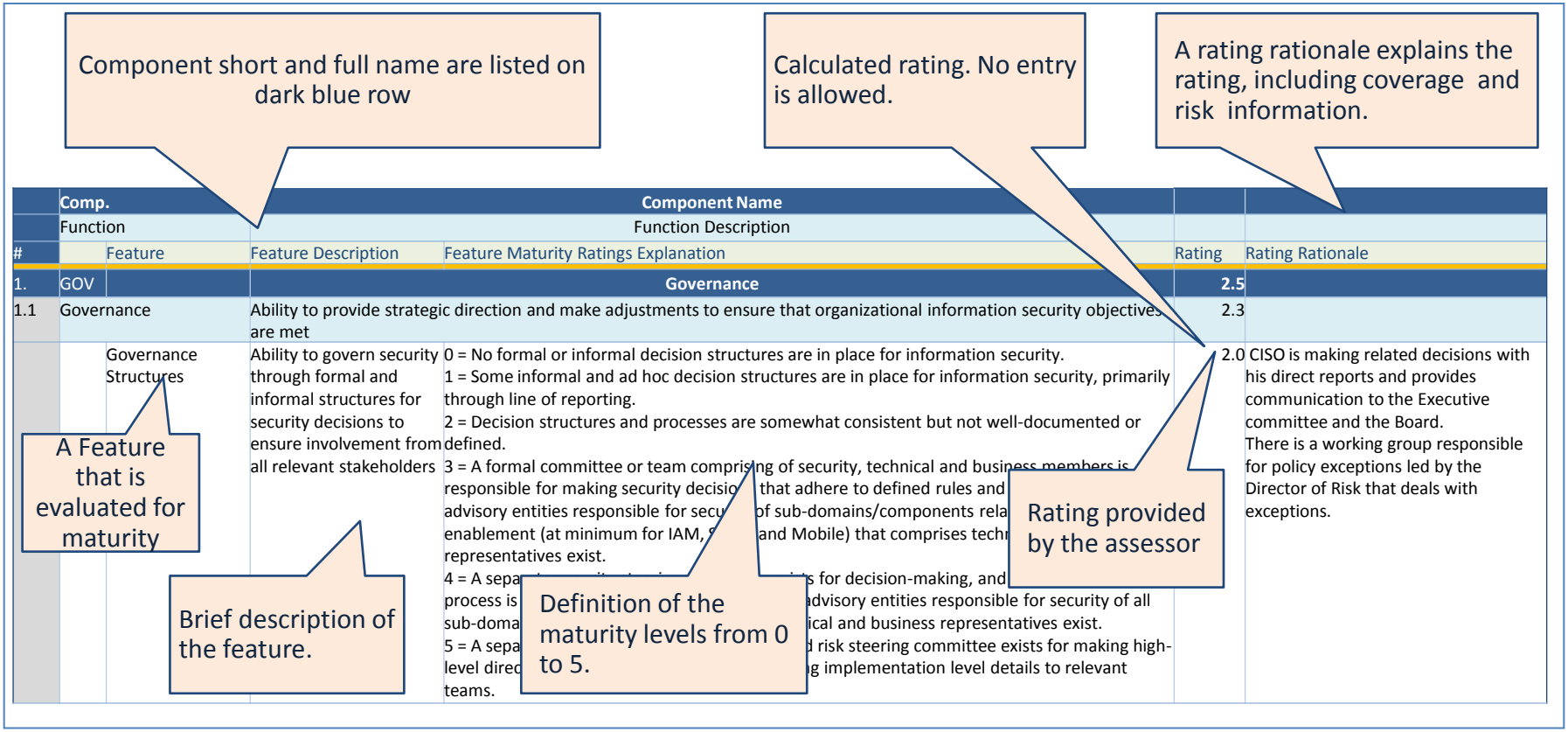
Security Capabilities & Components

- Four level structure/grouping:
  - Capability; strategic grouping of components
  - Component
  - Function
  - Feature
- Security maturity is assessed at the feature level,
  - component and function rating is automatically calculated based on the features rating
- Function maturity is calculated as an average of all related features
- Component maturity calculation:
  - Basic
  - Adjusted

#	Component Name	Short Name
1	Governance	GOV
2	Project Management	PM
3	Policy Program	POL
4	Mergers and Acquisitions	M&A
5	Audit / Compliance	A&C
6	System Placement (Sec Arch)	ARC
7	Awareness Training	AWA
8	Change Management	CHM
9	Vulnerability Management	VM
10	Application / DB Security	APP
11	End Point Protection	EPP
12	Data Loss Prevention	DLP
13	Cryptography	CRY
14	Security Monitoring	MON
15	Metrics	MET
16	Incident Response	IR
17	Network Perimeters & Zones	NET
18	Risk Management	RM
19	Information Classification	IC
20	Secure Development Lifecycle	SDL
21	Identity & Access Management	IAM
22	Mobile Security	MOB
23	Business Continuity Management	BCM

ISMM Assessment Tool

- Based on Excel.
- Features are evaluated on a zero to five scale with 0.5 increments.



#	Comp. Function	Feature	Feature Description	Feature Maturity Ratings Explanation	Rating	Rating Rationale
1.	GOV		**Governance**		**2.5**	
1.1	Governance		Ability to provide strategic direction and make adjustments to ensure that organizational information security objectives are met		2.3	
		Governance Structures	Ability to govern security through formal and informal structures for security decisions to ensure involvement from all relevant stakeholders	0 = No formal or informal decision structures are in place for information security. 1 = Some informal and ad hoc decision structures are in place for information security, primarily through line of reporting. 2 = Decision structures and processes are somewhat consistent but not well-documented or defined. 3 = A formal committee or team comprising of security, technical and business members is responsible for making security decisio that adhere to defined rules and advisory entities responsible for secu of sub-domains/components rela enablement (at minimum for IAM, and Mobile) that comprises techn representatives exist. 4 = A sepa s for decision-making, and process is dvisory entities responsible for security of all sub-doma ical and business representatives exist. 5 = A sepa d risk steering committee exists for making high-level direc g implementation level details to relevant teams.	2.0	CISO is making related decisions with his direct reports and provides communication to the Executive committee and the Board. There is a working group responsible for policy exceptions led by the Director of Risk that deals with exceptions.

Scoring and Rating Rationale

- Risk & Coverage Based Adjustments
  - Controls are rarely consistently implemented (coverage)
  - Not all assets are equally significant
  - Adjustments for Risk (focused on high-value/high-risk assets) & Coverage (applies to both processes and technologies)

		High Risk Systems/Apps.		
		76% - 100%	***51%-75%***	***25%-50%***
Coverage	***76%-100%***	0	-0.5	-1
	51%-75%	-0.5	-1	-1
	25%-50%	-1	-1	-1

- Rating rationale:
  - Supports the evaluation rating (reasoning)
  - List relevant people, processes, technologies/tools and environments considered
  - Think of it as data supporting past investments and information to build a business case for future investment in security capabilities

ISMM Adjustment Tool

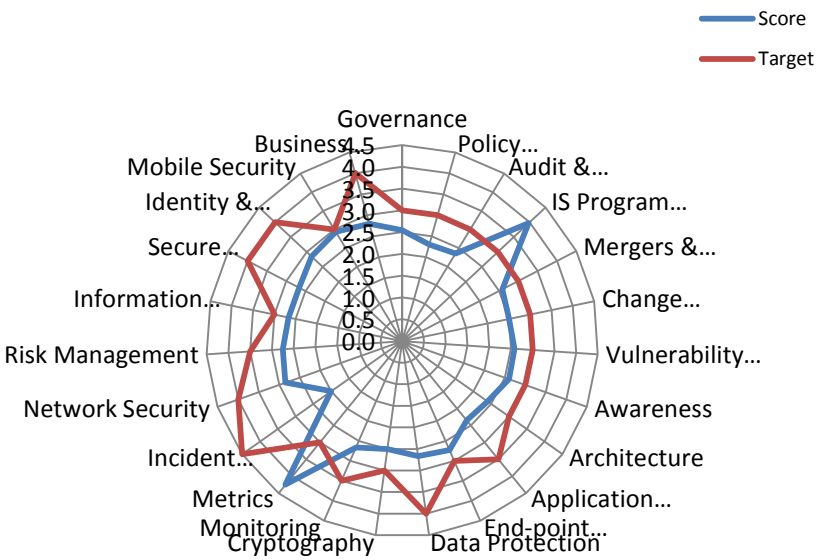
- Adjustments of the Basic Scores
  - adjusted based on perceived importance by the organization and component owners.
- Each of the Function is equally important (default)
- Customization
  - make some Functions more important, less important, or not applicable.
- No adjustments to Components
  - However, user can define through the Target Scores.

	Component			
	Function	Basic Score	Function Weight.	Adjusted Score
1.	Governance	**2.5**	**100**	**2.5**
1.1	Governance	2.3	10	
1.2	Strategy	2.8	25	
1.3	Security Innovation	2.5	15	
1.4	Security organization	2.4	25	
1.5	Business Relationship Management	2.5	25	
2.	Policy Management	**2.3**	**100**	**2.3**
2.1	Policy management	2.3	100	
3.	Audit & Compliance	**2.4**	**100**	**2.4**
3.1	Compliance management	1.9	50	
3.2	Audit and assurance	2.8	50	
4.	Program Management	**3.9**	**100**	**4.0**
4.1	IS Program Management	4.1	60	
4.2	Security Services Management	3.8	40	
5.	Mergers & Acquisitions	**2.6**	**100**	**2.6**
5.1	Mergers & Acquisitions	2.6	100	
10.	Application & Database Security	**2.6**	**ERROR**	**2.348**
10.1	Application Security	2.8	30	
10.2	Messaging & content security	2.4	30	
10.3	Databases	2.7	30	
11.	End Point Protection	**2.7**	**100**	**2.7**
11.1	Host Systems	2.8	50	
11.2	End-point	2.7	50	

ISMM Reporting

- Gaps
- Rationale
- Strategy adjustments and investment planning

#	Component	Component Description	Score	Target
1	GOV	Governance	2.5	3.0
2	POL	Policy Management	2.3	3.0
3	A&C	Audit & Compliance	2.4	3.0
4	PM	IS Program Management	4.0	3.0
5	MA	Mergers & Acquisitions	2.6	3.0
6	CHM	Change Management	2.5	3.0
7	VM	Vulnerability Management	2.6	3.0
8	AWA	Awareness	2.6	3.0
9	ARC	Architecture	2.4	3.0
10	APP	Application Security	2.3	3.5
11	EPP	End-point Security	2.7	3.0
12	DLP	Data Protection	2.7	4.0
13	CRY	Cryptography	2.5	3.0
14	MON	Monitoring	2.7	3.5
15	MET	Metrics	4.3	3.0
16	IR	Incident Response	2.0	4.5
17	NET	Network Security	2.9	4.0
18	RM	Risk Management	2.8	3.5
19	INF	Information Classification	2.7	3.0
20	SDL	Secure Development	2.7	4.0
21	IAM	Identity & Access management	2.9	4.0
22	MOB	Mobile Security	2.9	3.0
23	BCM	Business Continuity	2.8	4.0
		Overal IS Program Maturity	**2.72**	**3.35**



Note: All maturity data in this diagram is fictional

USING MATURITY MODELS FOR BUILDING STRATEGIES

Strategy is Both Art and Science

- Where we want to be and how to get there?
  - What are threats/risks?
  - What are available resources?
  - What are priorities?
  - What are specific projects/activities/schedule (Roadmap)
- Maturity models helps with the "science" part
  - Understand the baseline (where we are)
  - What's the gap?
  - Strengths and weaknesses
  - How we compare with the industry and competitors?
  - How to manage IS Portfolio?

#	Component Description	Score	Target
1	Governance	2.5	3.0
2	Policy Management	2.3	3.0
3	Audit & C	2.4	3.0
4	IS Progra	4.0	3.0
5	Mergers & Acquisitions	2.6	3.0
6	Change Management	2.5	3.0
7	Vulnerability Management	2.6	3.0
8	Awareness	2.6	3.0
9	Architecture	2.4	3.0
10	Application Security	2.3	3.5
11	End-point Security	2.7	3.0
12	Data Protection	2.7	4.0
13	Cryptography	2.5	3.0
14	Monitoring	2.7	3.5
15	Metrics	4.3	3.0
16	Incident Response	2.0	4.5
17	Network Security	2.9	4.0
18	Risk Management	2.8	3.5
19	Information Classification	2.7	3.0
20	Secure Development	2.7	4.0
21	Identity & Access management	2.9	4.0
22	Mobile Security	2.9	3.0
23	Business Continuity	2.8	4.0
	Overal IS Program Maturity	**2.72**	**3.35**

Note: All maturity data in this diagram is fictional

Some IS Strategy Options

Leveraging Maturity Models

- Start with understanding of:
  - High-risk/high value assets and related business objectives
  - Security threats/trends (e.g. build strong respond/recover capabilities)
  - Compliance requirements

- Some options to consider:
- If we know what others are doing (benchmarks available):
  - Just follow the industry (and peers) - stay within 0.5 to peers
  - Follow the industry but make sure we can recover quickly - be better in Monitoring and Incident Response capabilities and equal to industry in others
- If we don’t know what industry and our peers are doing
  - Address known issues and compliance
  - Chose to play on your strengths or reduce/eliminate weaknesses

Final Thoughts on Maturity Models & Strategy

- You may need some planning to get your favorite coffee, but
- Climbing Mt. Everest is something different! It requires serious planning, developing climbing capabilities, agility to make strategy changes, communications and program overall support.

Start at the Base Camp

Overcome the obstacles (threats) through camps I, II, III and IV

Climb the Summit!

QUESTIONS?

Thank you!

Goran Kovacevic, gorkovac@visa.com