

PART 1 of 2

Insight into Security Leader Success

*How to get the Enterprise to
Understand the Value of Security*

A SEC Research Finding



Intended Audience

This presentation is intended for security leaders who want to create a **business-based** security department that **provides value**, and is **valued by the enterprise**.

The following recommendations are based on **10+** years of SEC relevancy-based research.

Dear viewer,

Senior management is basing their decisions more and more on factual data and research – they're demanding better answers. We are finding this trend is reaching into the realm of Security in an ever increasing number of organizations.

The following recommendations are based on our interactions with, and research on, security programs and practitioners.

We believe the findings expressed in this presentation are the minimum requirements for successful security practitioners.

Sincerely,

SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Expectations Are Changing

Old Expectations

New Expectations

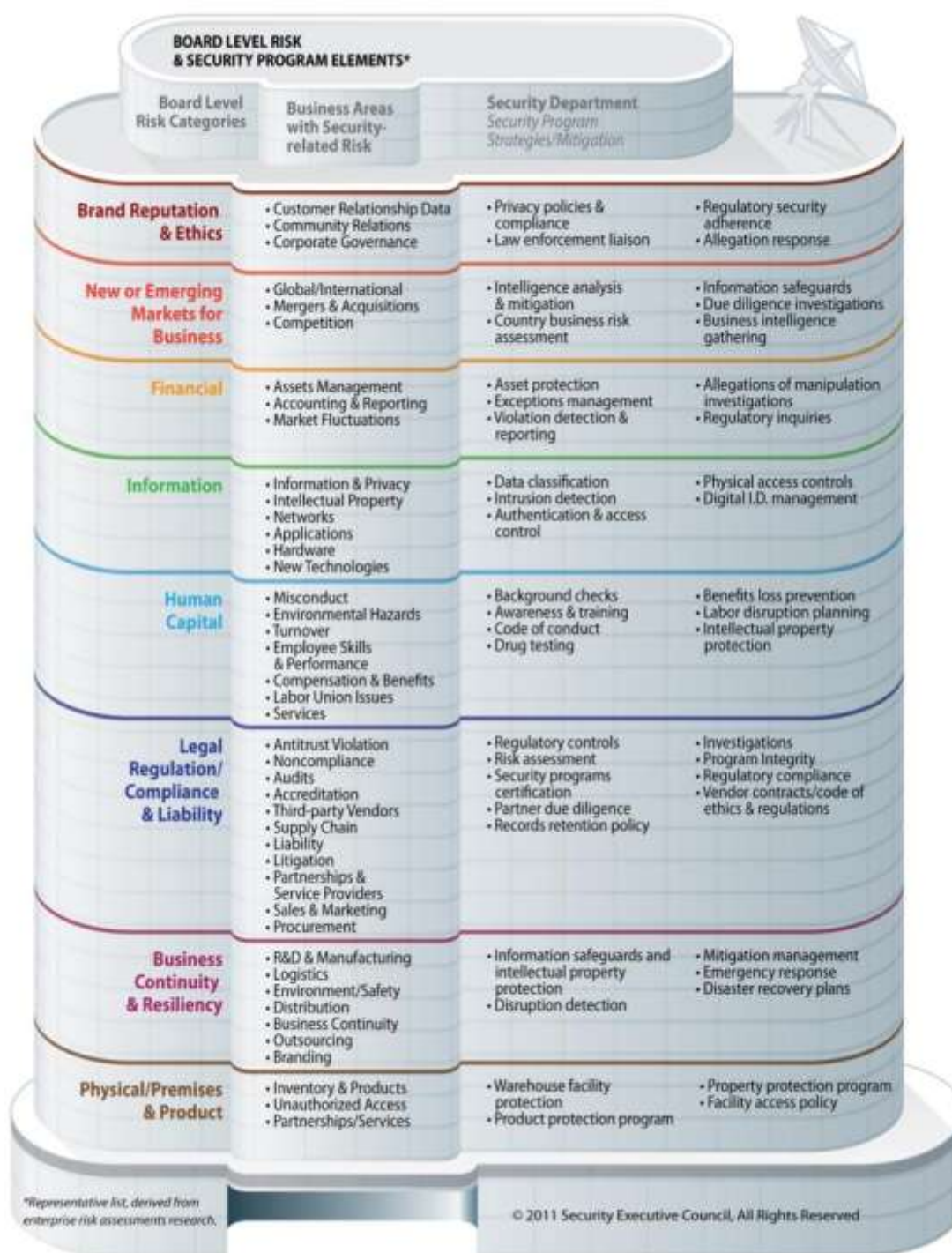


What does it take to meet
the NEW expectations?



1

Be Risk Based & Aligned with Organizational Goals



Are your programs based on risks agreed upon across the enterprise?

Are you using the same language the Board uses to express these risks?

When and where does Security mitigate those risks?



Enterprise and Security Risk Alignment – key points to know.

Define the relationship between your company's strategic business objectives and the alignment of risk mitigation and security programs.



Enterprise and Security Risk Alignment – key points you need to know.

Adjust security program creation to match vulnerabilities and threats (risks) identified with the future direction of the company. The greater the alignment between the goals of the business units and the security programs developed to support these goals, the greater the success of the company and the security leader.



Enterprise and Security Risk Alignment – key points you need to know.

Delineate the structural issues surrounding the development of security programs, including program maturity, cost considerations, emerging risks and a growing body of regulatory and compliance issues.

Have you conducted a security risk/threat/vulnerability assessment?



If not...

WHY NOT???

Would you start fixing a car before knowing what's potentially wrong with it?

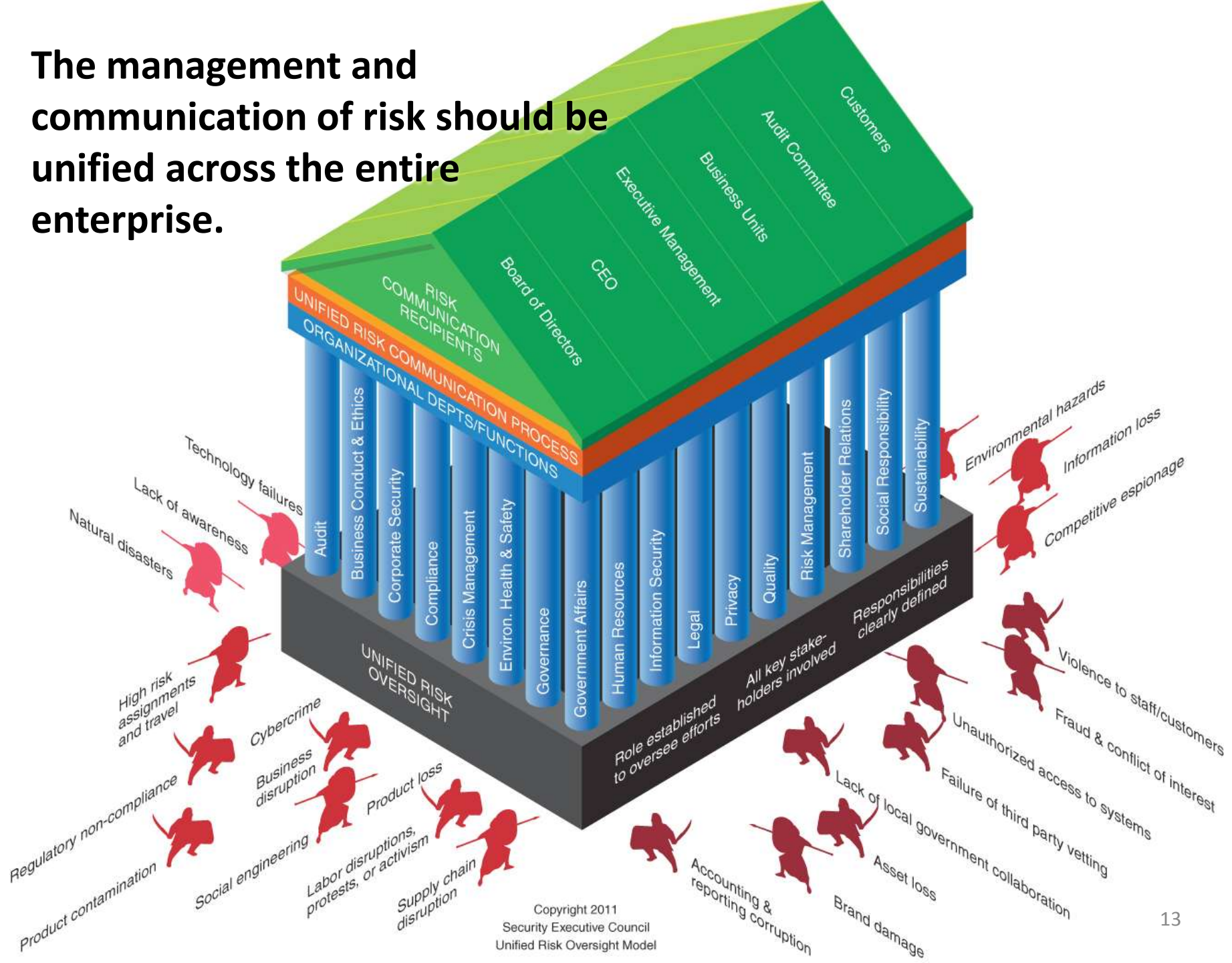
If you have - do you regularly re-assess?



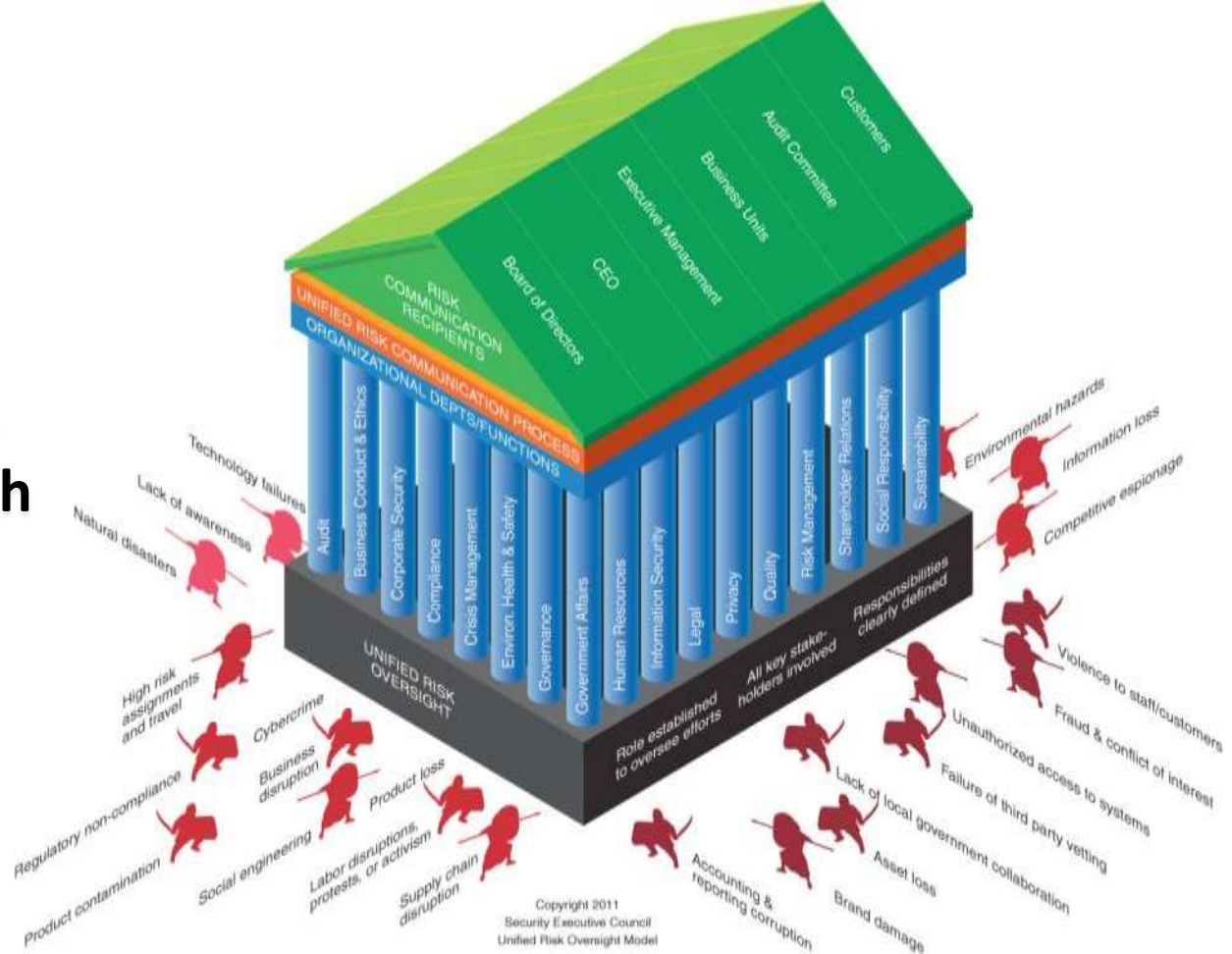
2

Influence Cross-Functional Teams

The management and communication of risk should be unified across the entire enterprise.

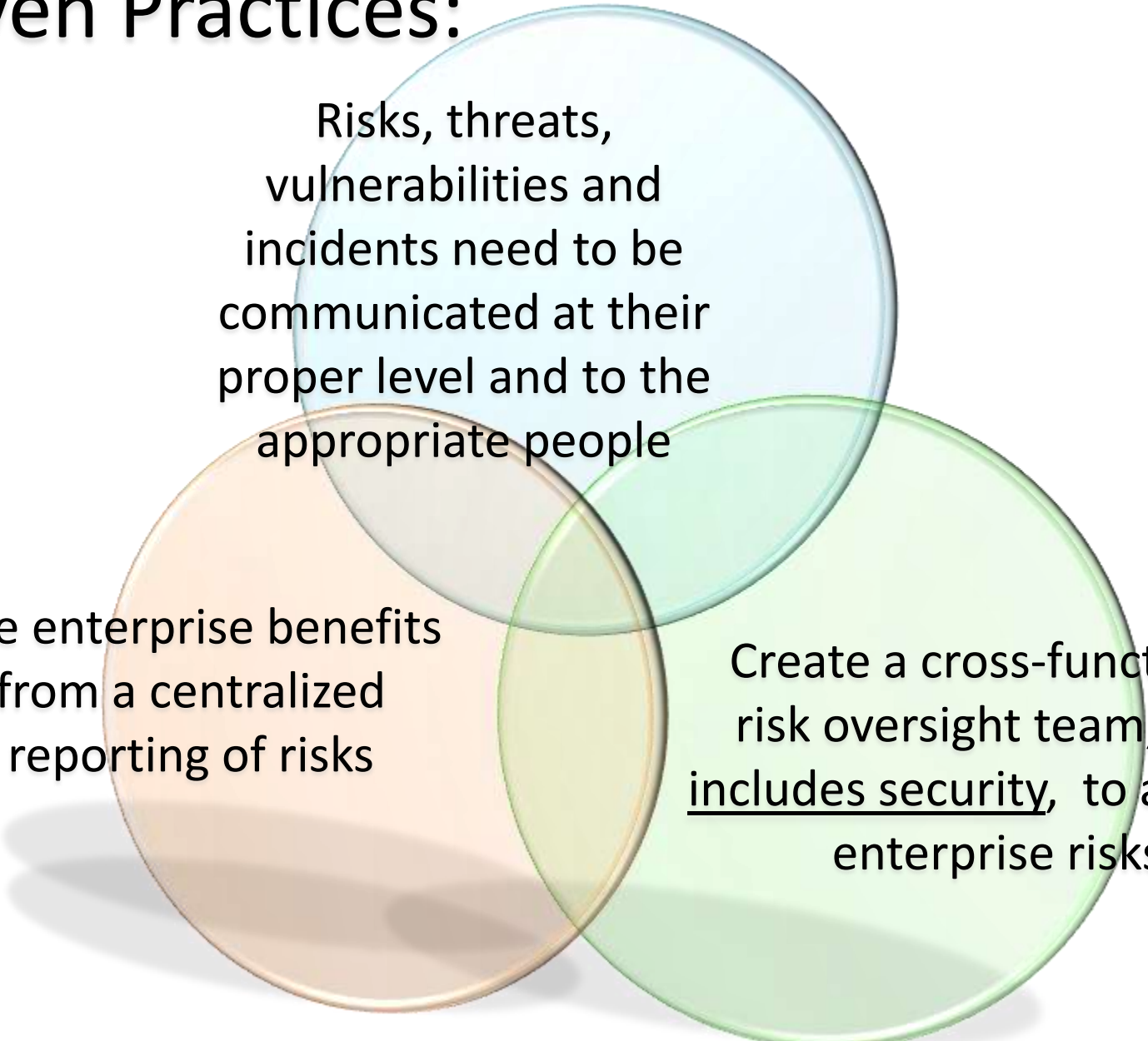


Most organizations address risk through separate and uncoordinated functional areas.



We think Security can help bridge these silos of risk.

Proven Practices:



Risks, threats,
vulnerabilities and
incidents need to be
communicated at their
proper level and to the
appropriate people

The enterprise benefits
from a centralized
reporting of risks

Create a cross-functional
risk oversight team, that
includes security, to address
enterprise risks



3

Security is Aligned with Organizational Readiness

Organizational Readiness and OPaL+

First, What is OPaL+?

The SEC conducted extensive research that focused on when and how Security programs and people become valued by the enterprise.

This research found critical elements that when aligned properly result in a Security department that is a fit for and greatly valued by the enterprise.

These elements are:

Organizational readiness

Program Maturity

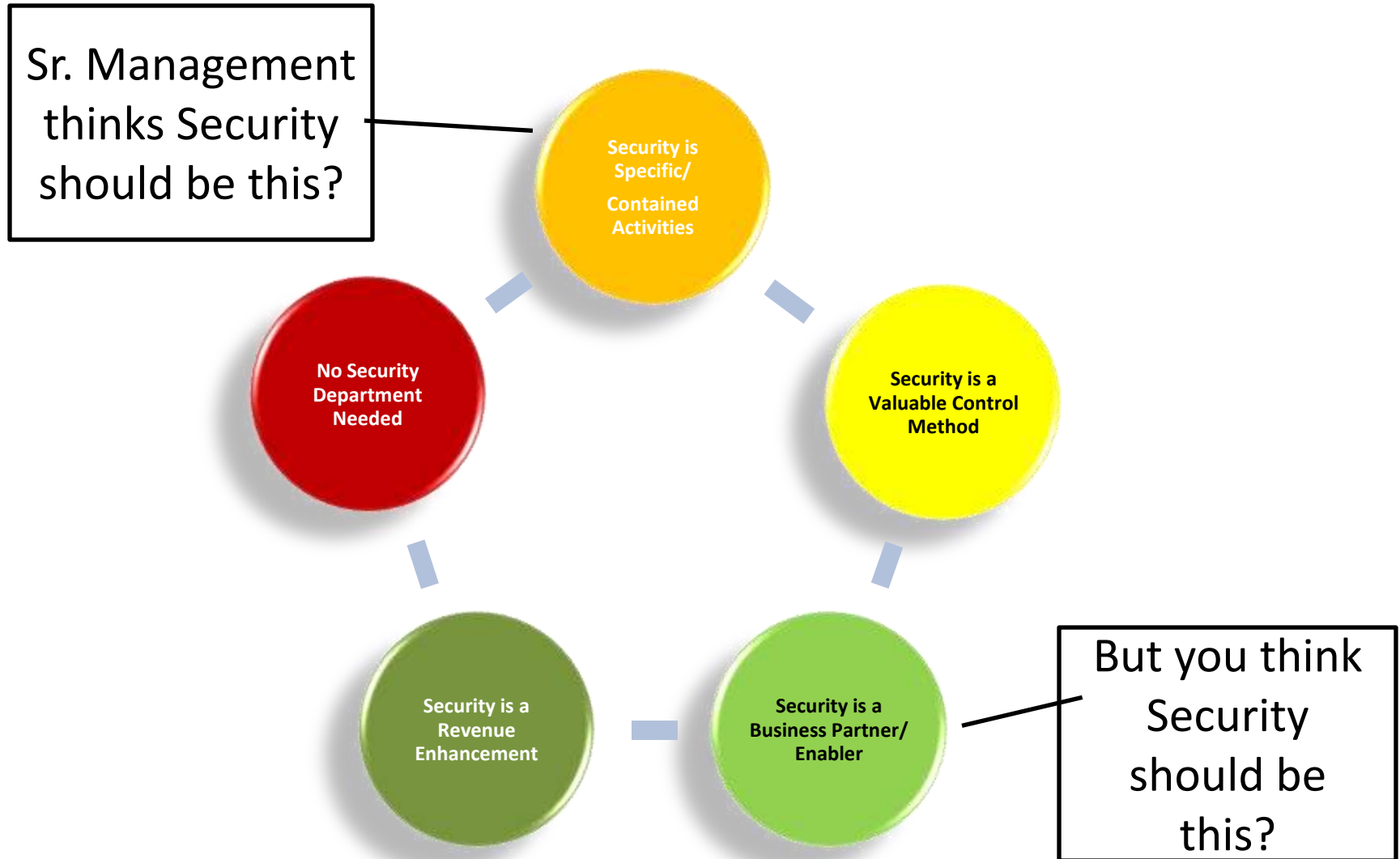
Leadership Continuum

+

Organizational elements of Corporate Culture and Risk Appetite



Organizational readiness refers to whether the organization is “ready” for Security’s blueprint.



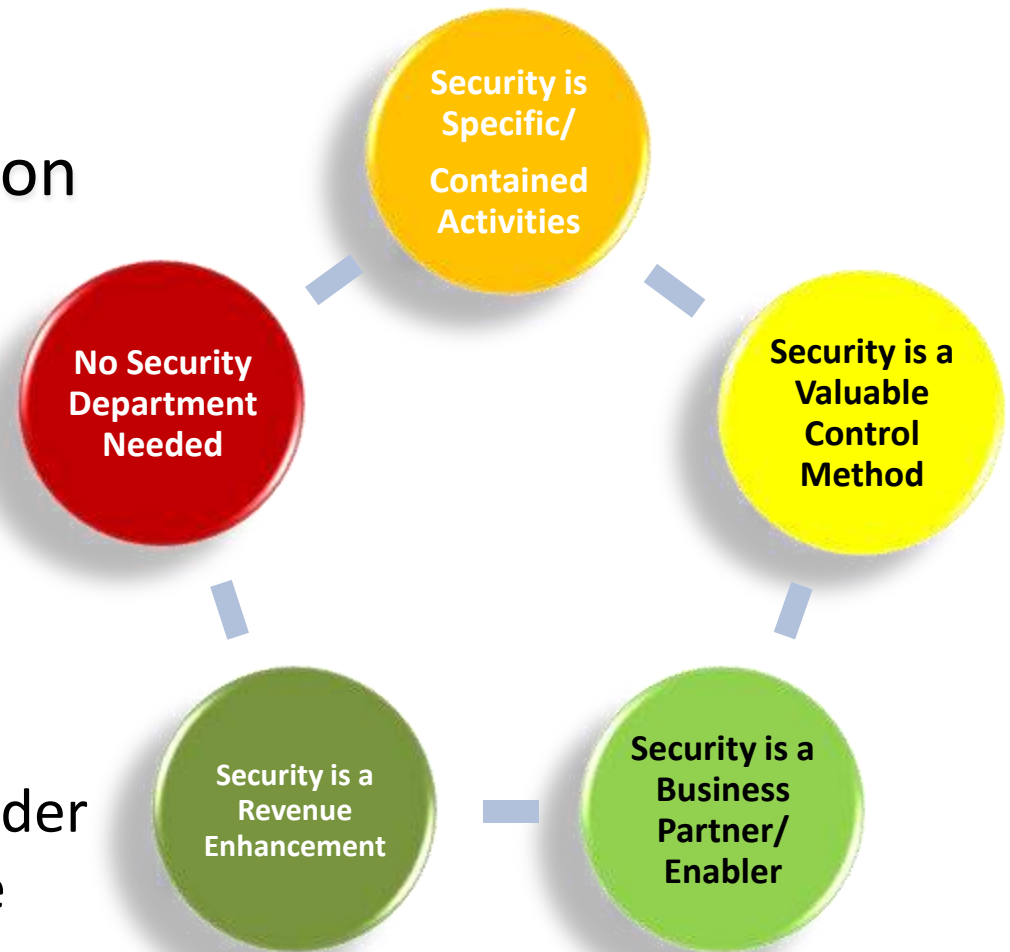
Understanding *Organizational Readiness* ensures that the organization and Security agree as to what Security should be and what it should accomplish.

If there is a lack of agreement then expectations will be misaligned.



You can enhance your cohesion with organization expectations by:

- ✓ Aligning with your organization's corporate culture
- ✓ Being the right type of leader for the organization at the right time



- ✓ Coming to an agreement with the organization on the current maturity level of security programs and creating a plan from there to the next level



4

Create the Security Regulatory/Standards Baseline

Item	Acronym	Creation	Name	Dsp	URL
26	Legislation	EO12958	Executive Order 12958 - Information Sharing	Y	www.archives.gov
27	Legislation	EO13224	Executive Order 13224 - Doing Business w/ Terrorists	Y	www.vawinter.com
28	Legislation	EO13231	Executive Order 13231 - Infrastructure Protection	Y	www.ncs.gov
29	Legislation	EO13234	Executive Order 13234 - Citizen Preparedness	Y	www.emergency-management.net
30	Legislation	NSPD-2	Presidential Directive 2	Y	www.fas.org
31	Legislation	HSPD-3	Presidential Directive 3	Y	www.dhs.gov
32	Legislation	HSPD-7	Presidential Directive 7	Y	www.dhs.gov
33	Legislation	HSPD-8	Presidential Directive 8	Y	www.dhs.gov
34	Legislation		Homeland Security Act	Y	frwebgate.access.gpo.gov
35	Legislation		Transportation Security Act	Y	frwebgate.access.gpo.gov
36	Legislation		Customs Modernization Act	Y	www.govexec.com
37	Legislation		Security Enhancement Act of 2002	Y	www4.law.cornell.edu
38	Legislation		Federal Anti-Tampering Act	Y	www.fda.gov
39	Legislation		Materials Law	Y	www.phmsa.dot.gov
40	Legislation		Foreign Corrupt Practices Act	Y	www.worldcompliance.com
41	Legislation		Emergency Economic Powers Act	Y	www4.law.cornell.edu
42	Legislation		Maritime Transportation Security Act of 2002	Y	www4.law.cornell.edu
43	Legislation		Information Infrastructure Protection Act	Y	www.usca.mil
44	Legislation		Notification and Federal Emergency Management Agency Act	Y	www4.law.cornell.edu
45	Legislation		Public Health Security and Bioterrorism Preparedness & Response Act of 2002	Y	frwebgate.access.gpo.gov
46	Regulation		USA PATRIOT Act	Y	www.fda.gov
47	Regulation		USA PATRIOT Act	Y	frwebgate.access.gpo.gov
48	Regulation		USA PATRIOT Act	Y	frwebgate.access.gpo.gov
49	Regulation		USA PATRIOT Act	Y	frwebgate.access.gpo.gov
50	Regulation		USA PATRIOT Act	Y	www.csrees.usda.gov
51	Regulation		USA PATRIOT Act	Y	www.tsa.gov
52	Regulation		USA PATRIOT Act	Y	www.tsa.gov
53	Regulation		USA PATRIOT Act	Y	www.tsa.gov
54	Regulation		USA PATRIOT Act	Y	www.tsa.gov
55	Regulation		USA PATRIOT Act	Y	www.tsa.gov

Just a sample of regulations and standards around or with security aspects.



- AEO**
- C-TPAT**
- FISMA**
- GLBA**
- SOX**
- PCI**
- NERC-CIP**
- HIPAA**
- NFPA 1600**
- ISO 27001**
- CFATS**
- FSMA Food Safety Modernization Act**
- MARSEC**
- European Union Data Protection Directive**
- NIST**
- ISO 22399**

Using the Security Regulatory/Standards Baseline



- ➔ Integrate global compliance standards and system specifications**
- ➔ Expedite and optimize fixed cost (security personnel and systems) investment and variable cost outcomes (injury, asset damage or loss)**
- ➔ Provide for common denominator audit guidance for security requirements including self-assessments**



5

Operate Security like a Business

When running Security like a business, you should be able to easily answer the following questions:

Who are your internal **customers**? What motivates them? What services do they use? What do they value? How confident are they in your services?

What **product** do you “sell?” Have you identified all of your security services? What risks do they specifically reduce? How do you measure their business value?

What is your **capacity**? How much time do staff devote to each kind of activity? What is the cost per service?

What is your “**marketing strategy**” for the security department? What is your brand image to the company?



This concludes part 1 of *Insight into Security Leader Success*.

This presentation (parts 1 and 2) incorporates aspects of the following SEC developed research and content from the SEC Corporate Security Knowledge Base:

- Board-Level Risk Model
- Enterprise/Security Risk Alignment Model
- Unified Risk Oversight Model
- 9 Practice of the Successful Security Leader Research
- OPaL+ Assessment Research
- Security Measures and Metrics Program
- Internal Valuation Assessment Model
- Next Generation Security Leader Program
- Running Security as a Business Research
- Regulation and Compliance Management Database
- Executive Management Communication Best Practices
- SEC Technology Roadmap

And the collective knowledge of SEC staff and subject matter experts (former security executives and security industry leaders)



We can bring our research and extensive experience to work with you on:

- Aligning security risk mitigation strategies with enterprise risks
- Assessing risks, threats and vulnerabilities
- Creating your value driven metrics program
- Developing and telling Security's story
- Becoming a part of the business-wide risk team
- Aligning organizational readiness, program maturity and leadership strategy
- Contributing to enterprise driven risk compliance
- Running a business-based Security operation
- Transforming the Security organization through powerful executive communication

Contact us. We're a security risk mitigation research and advisory firm. We're made up of former successful security executives. We enjoy exploring how to make Security a valued part of the business.

contact@seclader.com

+1 202.730.9971

<https://www.securityexecutivecouncil.com>

