Advancing Information Risk Practices

Start Time	Title	Presenter
1:00 PM	Assessment Pitfalls for Risk Managers	Jeff Lowder
1:55 PM	It's Not All Academic: A Case Study Implementing Cyber Risk Management	Summer Fowler
2:45 PM	BREAK	
3:00 PM	Managing Third-Party Risk	Evan Wheeler, Scott Andersen, Julie Fitton, Brad Keller, Irfan Saif
3:40 PM	Architectural Risk Analysis: NIST 800-53 on Steroids	Evan Wheeler

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Assessment Pitfalls for Risk Managers

SESSION ID: SEM-M03

Jeff Lowder

Director, Global Information Security and Privacy
OpenMarket
@agilesecurity

Is Information Risk Management Feasible?

No!

- Donn Parker

- Marcus Ranum

Yes!

- George Westerman and Richard Hunter

- Doug Hubbard

Audience Poll

- Is Information Risk Analysis **Quantitive** or **Qualitative**?

Correct Answer

Correct Answer: BOTH.

- **Quantitative**: has to do with numerical quantities
- **Qualitative**: deals with qualities or characteristics, not numerical quantities

Qualitative & Quantitative Aspects

IRM Quantitative Aspects

- Probability *Value*
- Business Impact *Amount*
- Risk Treatment *Cost*
- Risk Reduction *Amount*
- Risk *Velocity*

IRM Qualitative Aspects

- Probability *Type*
- Business Impact *Types*
- Risk Treatment *Decision*
- Risk *Owner*
- Risk *Viewpoint*

Risk Estimation

Quick Check: How Good Are You at Estimating Risk?

- Even if you don’t know the exact value of something, you can usually estimate a range of values!
- How good do you think you are you at estimating ranges? How do you know?
- Find out! Take a quick calibration survey.

Calibration Survey

#	Question	Answer
1	How many feet tall is the Hoover Dam?	
2	How many inches long is a $20 bill?	
3	What % of aluminum is recycled in the U.S.?	
4	When was Elvis Presley born?	
5	What percentage of the atmosphere is oxygen by weight?	

Calibration Survey

#	Question	Answer
6	What is the latitude of New Orleans?	
7	In 1913, the U.S. military owned how many airplanes?	
8	The first European printing press was invented in what year?	
9	What % of all electricity consumed in U.S. households was used by kitchen appliances in 2001?	
10	How many miles tall is Mt. Everest?	

How did you do? Answers for calibration survey

#	Question	Answer
1	How many feet tall is the Hoover Dam?	738
2	How many inches long is a $20 bill?	63/16ths (6.1875)
3	What % of aluminum is recycled in the U.S.?	45%
4	When was Elvis Presley born?	1935
5	What percentage of the atmosphere is oxygen by weight?	21%

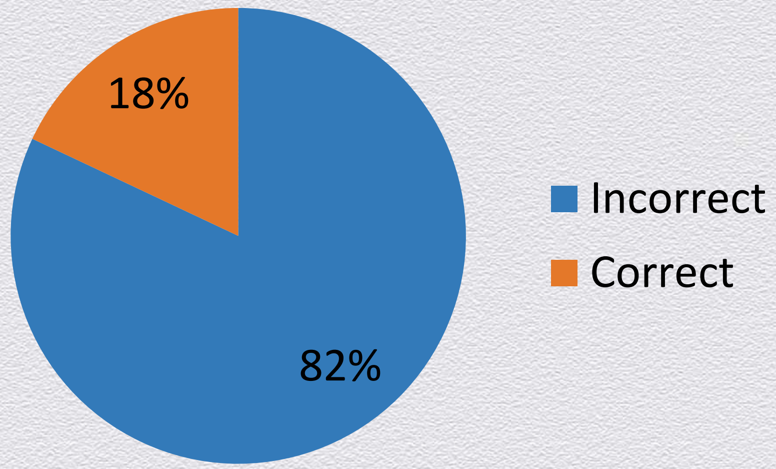
How did you do? Answers for calibration survey

#	Question	Answer
6	What is the latitude of New Orleans?	31
7	In 1913, the U.S. military owned how many airplanes?	23
8	The first European printing press was invented in what year?	1450
9	What % of all electricity consumed in U.S. households was used by kitchen appliances in 2001?	26.7%
10	How many miles tall is Mt. Everest?	5.5

How Did Your Peers Do?

Lowder's Research:

- How often do GRC professionals correctly estimate ranges in their 90% CI?
  - Among GRC professionals responsible for implementing IRM, the percentage of correct responses dropped to 10%



Quick Check: How Good Are You at Estimating Risk?

- The proportion of vulnerabilities in the **HackMe Operating System** with publicly available exploit code is 80%.
- The proportion of vulnerabilities in the **Fort Knox Operating System** with publicly available exploit code is 10%.
- A new **HackMe** vulnerability is announced with a CVSS score of 6.0.
- A new **FortKnox** vulnerability is announced with a CVSS score of 8.0.
- Which vulnerability should you remediate first?

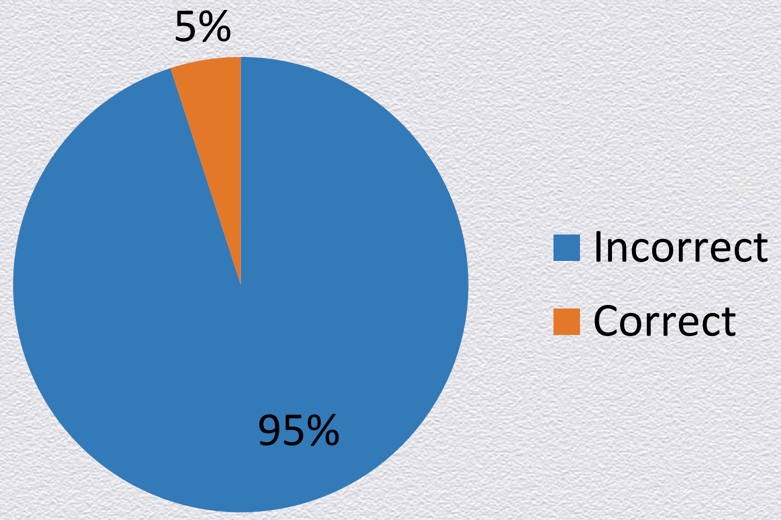
Correct Answer

- The **HackMe** vulnerability.

How Did Your Peers Do?

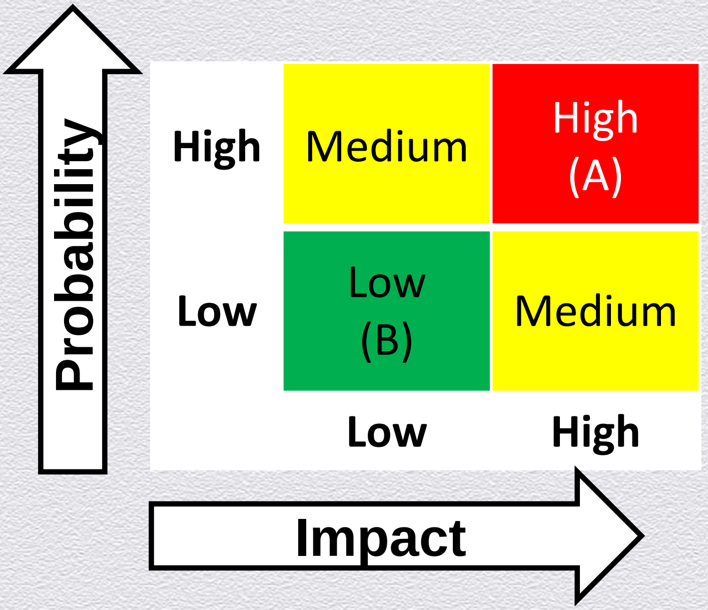
Lowder's Research:

- How often do GRC professionals commit the base-rate fallacy?
  - When presented with conditional probabilities, 95% of GRC professionals commit the base-rate fallacy



Audience Poll

- How many of you use a **High / Medium / Low** scale for probability, frequency, impact, or risk?

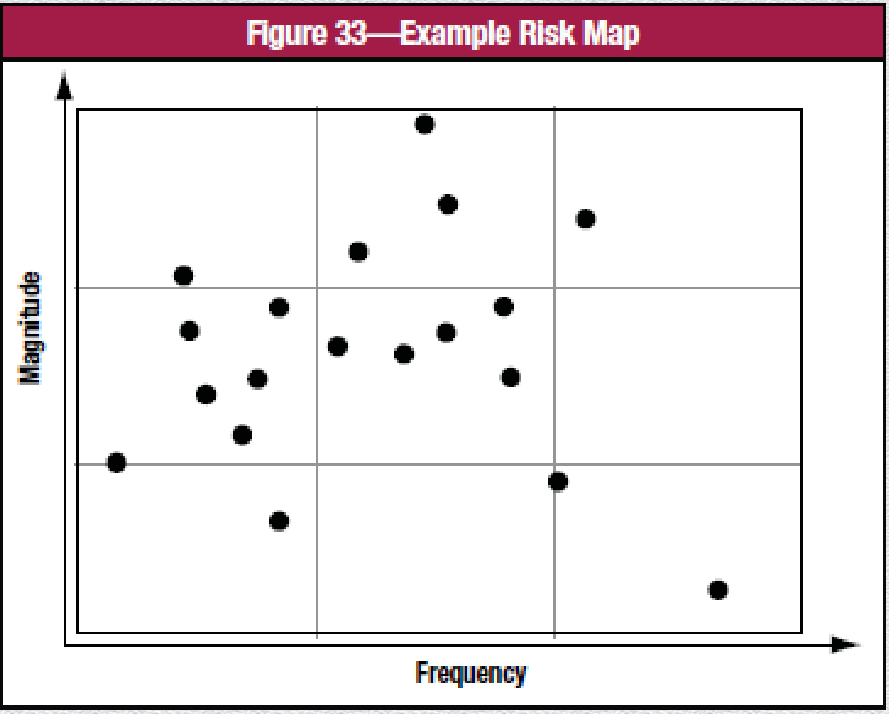


Probability

High	Medium	High (A)
Low	Low (B)	Medium
	Low	**High**

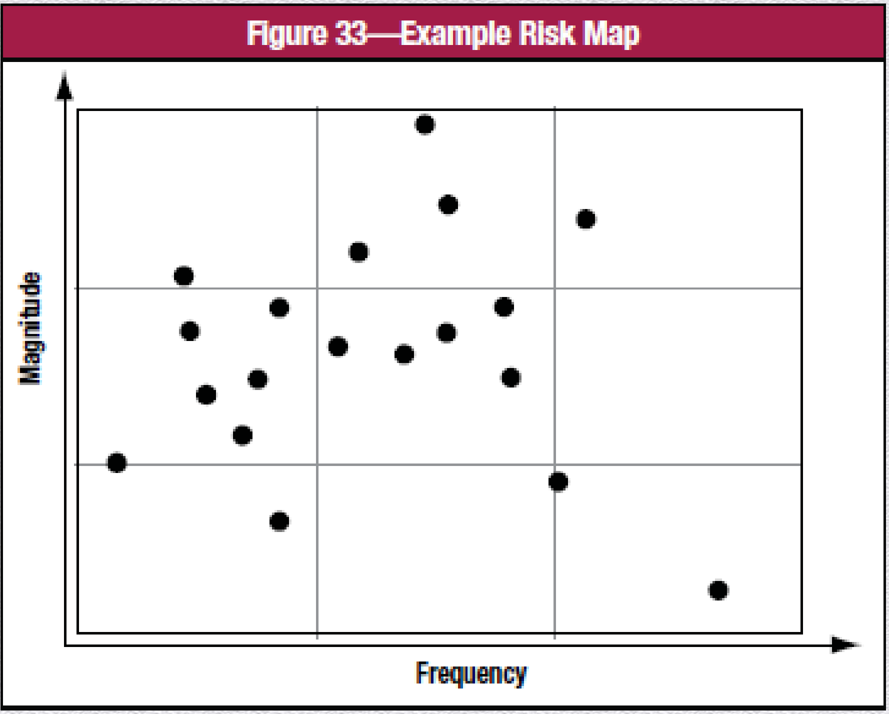
Impact

Audience Poll



Have you ever produced a matrix like this?

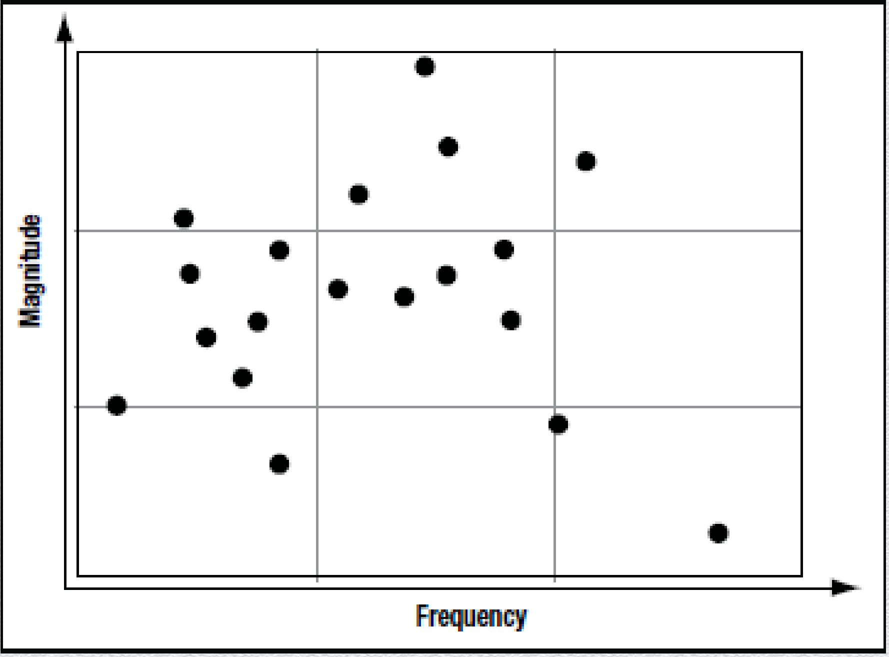
Audience Poll



Have you ever ‘moved’ the dots around inside a cell?

The Bad News

Figure 33—Example Risk Map



You can't do that.

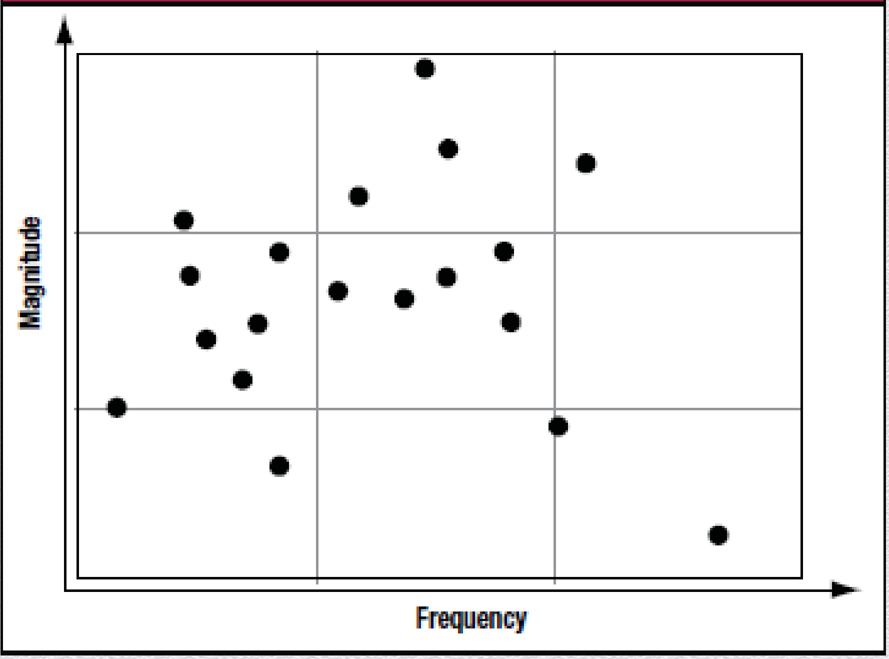
Scales of Measure

- **Nominal Scale**: used only for identification; does not indicate quantity, rank, or any other measurement.
- **Ordinal Scale**: used to denote a position in an ordered sequence (e.g., first, second, third, fourth).
- **Interval Scale**: used to define the distance between two ordinal numbers.
- **Ratio Scale**: used to express proportion.

OpenMarket

The Bad News

Figure 33—Example Risk Map

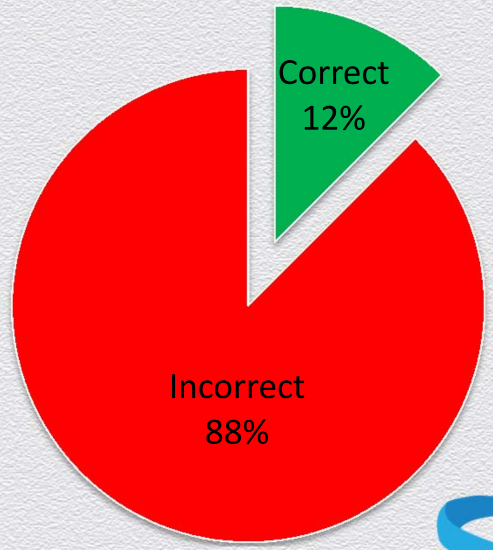


An ordinal scale **cannot** tell you where to put the dots inside the boxes in this matrix

Ordinal Scales + Risk Matrices = Bad Combo

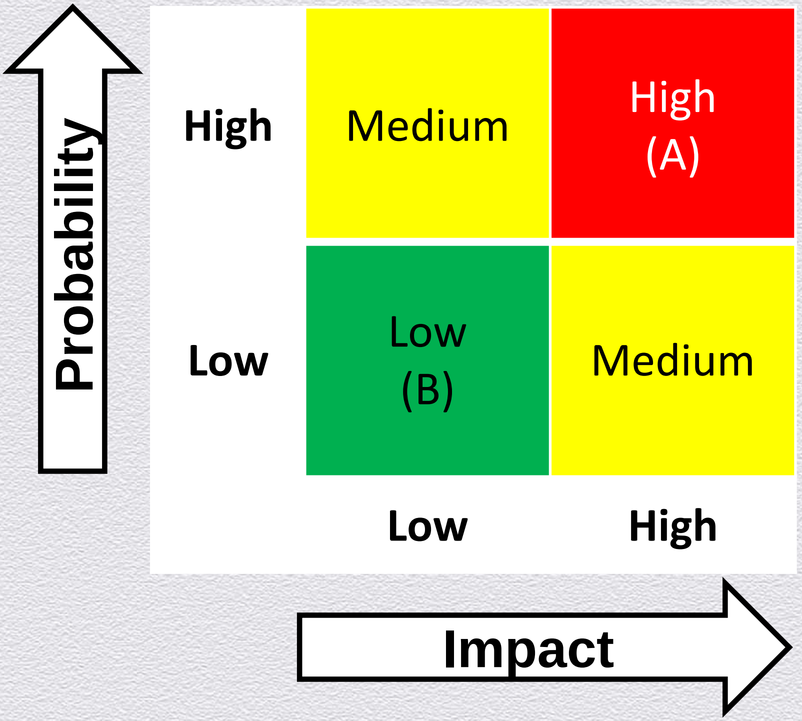
Tony Cox, Ph.D., Risk Analysis

"Risk matrices [***plus ordinal scales***] can be ***worse than useless*** for High-Low and Low-High risks."



Analysis: 2 x 2 Risk Matrix

Scenario 1



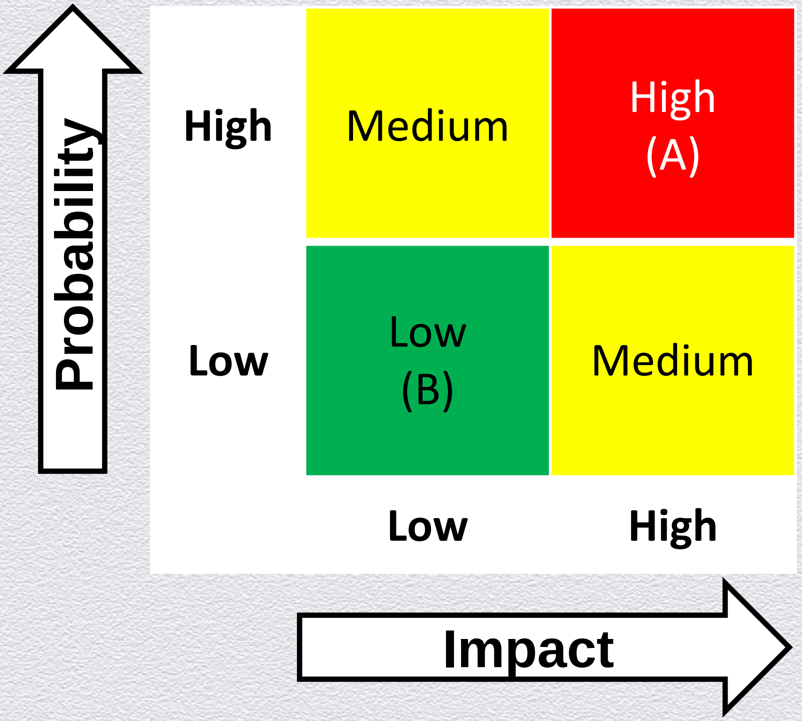
	Low	High
High	Medium	High (A)
Low	Low (B)	Medium

If A is high and B is low (or vice versa), the two risks can be ranked with no error.

The probability of this is (1/2) * (1/4) = **0.125.**

Analysis: 2 x 2 Risk Matrix

Scenario 2



	Low	High
High	Medium	High (A)
Low	Low (B)	Medium

Probability

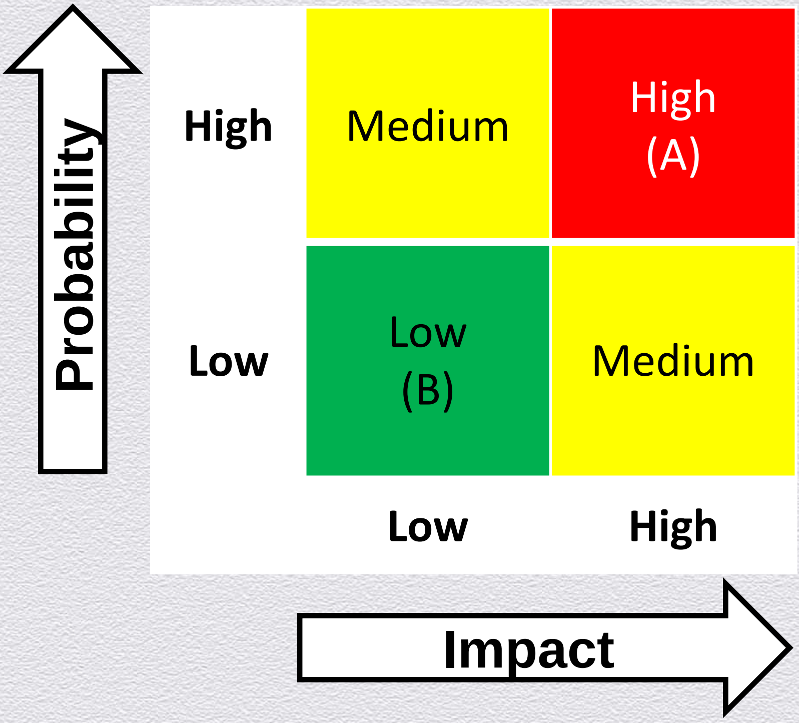
Impact

If both A and B have the same rating, the risk matrix provides no way to choose among them.

The probability of this is (1/4) * [(1/2) + (1/4) + (1/2) + (1/4)] = 0.375.

Analysis: 2 x 2 Risk Matrix

Scenario 3



	Low	High
High	Medium	High (A)
Low	Low (B)	Medium

Probability

Impact

If one risk is medium and the other is not, sometimes the risk matrix will incorrectly rank the risks.

The probability of this is 1 – 0.125 – 0.375 = 0.5.

Analysis: 2 x 2 Risk Matrix

Scenario	Accurate?	Probability
1	☺	12.5%
2	☺ / ☹	37.5%
3	☺ / ☹	50%

What Does This Mean?

Risk Matric Outcome	Probability
Erroneous Risk Matrix	87.5%
No Better than Flipping a Coin	37.5%

For More Information

- Information Risk Management Body of Knowledge (IRMBOK™)
  - Society for Information Risk Analysts
  - www.societyinforisk.org
  - @societyinforisk

Advancing Information Risk Practices

Start Time	Title	Presenter
1:00 PM	Assessment Pitfalls for Risk Managers	Jeff Lowder
1:55 PM	It's Not All Academic: A Case Study Implementing Cyber Risk Management	Summer Fowler
2:45 PM	BREAK	
3:00 PM	Managing Third-Party Risk	Evan Wheeler, Scott Andersen, Julie Fitton, Brad Keller, Irfan Saif
3:40 PM	Architectural Risk Analysis: NIST 800-53 on Steroids	Evan Wheeler

RSA®CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

It's Not All Academic: A Case Study on Implementing a Cyber Risk Management Program

SESSION ID: SEM-M03

Summer Craze Fowler

Deputy Director Cyber Security Solutions (CS2)
Carnegie Mellon University’s Software Engineering Institute (CERT Division)
@sumfowler

Advancing Information Risk Practices

Start Time	Title	Presenter
1:00 PM	Assessment Pitfalls for Risk Managers	Jeff Lowder
1:55 PM	It's Not All Academic: A Case Study Implementing Cyber Risk Management	Summer Fowler
2:45 PM	BREAK	
3:00 PM	Managing Third-Party Risk	Evan Wheeler, Scott Andersen, Julie Fitton, Brad Keller, Irfan Saif
3:40 PM	Architectural Risk Analysis: NIST 800-53 on Steroids	Evan Wheeler

RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Managing Third-Party Risk

SESSION ID: SEM-M03

Brad Keller
The Santa Fe Group

Irfan Saif
Deloitte & Touche LLP

Evan Wheeler
Omgeo

Julie Fitton
EMC Corporation

Scott Andersen
Citi

Advancing Information Risk Practices

Start Time	Title	Presenter
1:00 PM	Assessment Pitfalls for Risk Managers	Jeff Lowder
1:55 PM	It's Not All Academic: A Case Study Implementing Cyber Risk Management	Summer Fowler
2:45 PM	BREAK	
3:00 PM	Managing Third-Party Risk	Evan Wheeler, Scott Andersen, Julie Fitton, Brad Keller, Irfan Saif
3:40 PM	Architectural Risk Analysis: NIST 800-53 on Steroids	Evan Wheeler

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Architectural Risk Analysis: NIST 800-53 on Steroids

SESSION ID: SEM-M03

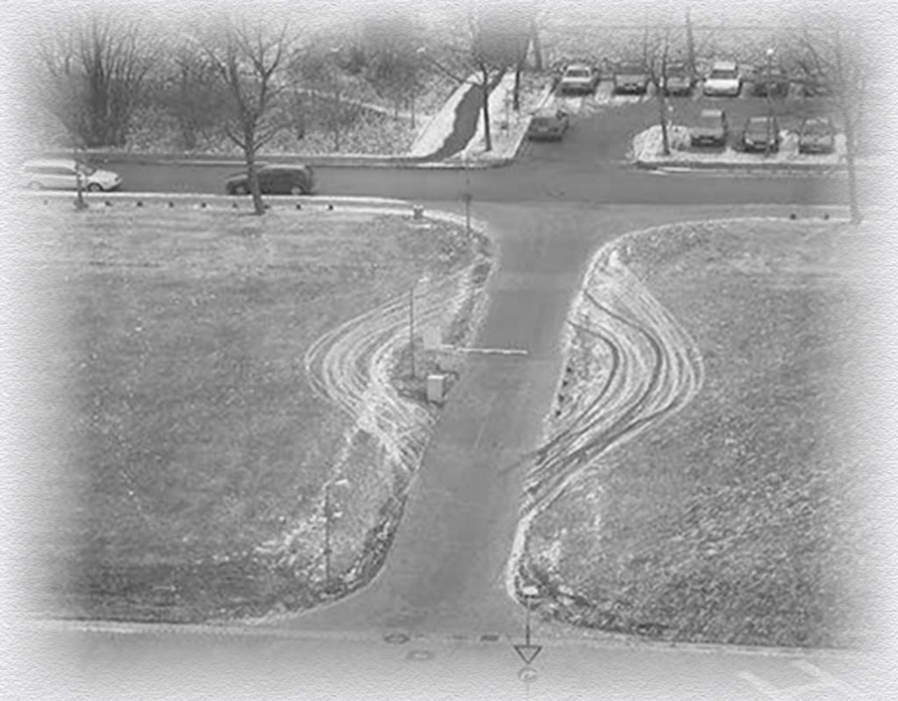
Evan Wheeler

Director, IT Risk Management

Topics

- Starting with requirements, not just controls
- Analyzing information flows
- Leveraging trust models
- Reducing the threat surface
- Establishing reusable patterns
- Scenario:
  - Designing an alpha testing environment for Agile development team

Are your controls tailored to your organization?



#RSAC

RSΛCONFERENCE2014

Assume Nothing

“Design flaws account for 50% of security problems. You can’t find design defects by staring at code — a higher-level understanding is required.”

- Gary McGraw

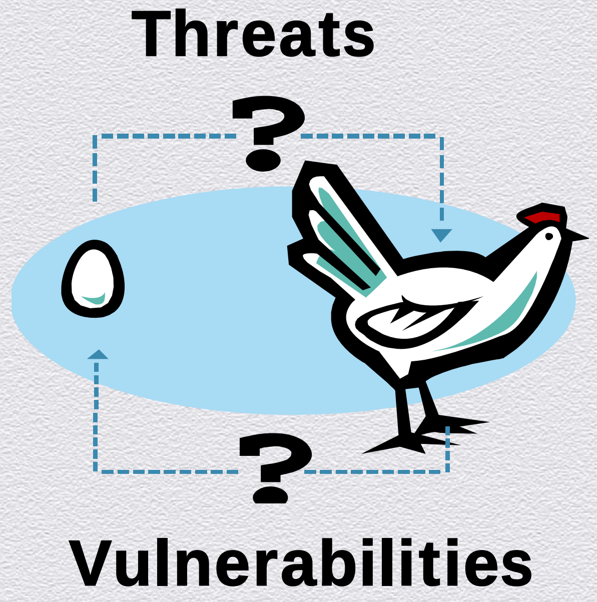
Three fundamental assessment activities:

1. Penetration Testing
2. Code Reviews
3. Architectural Risk Analysis

Source: *Software Security: Building Security In*

Where do you start assessing?

1. Business Impact Assessment
2. Threat Modeling
3. Incident/Vulnerability Analysis
4. Controls Self Assessment



Case Study - AcmeHealth

- AcmeHealth based in Cambridge, MA
- A medium sized healthcare benefits software provider
- Provides hosted benefits management solution
- Customers located in all 50 states and 16 countries
- Company has about 150 fulltime employees

AcmeHealth Scenario – Alpha Environment

- Company is moving to an Agile development model
- Development team is asking to create an alpha environment for testing functionality with customers
- Business requirements:
  - Needs to be Internet accessible
  - Will have no real data, just test data
  - Will often have code that has only been functionally tested
  - Internal access needs to be open and flexible

RSA CONFERENCE 2014

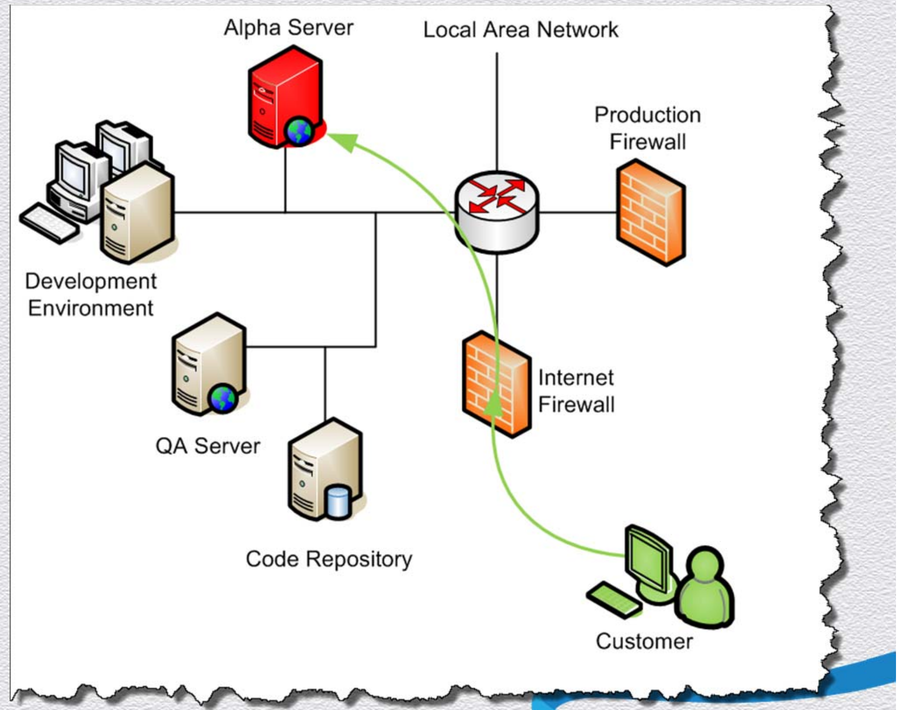
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Sensitivity & Threats

AcmeHealth Proposal for Development Team

Dev Proposal

- Add new alpha server to existing DEV/QA network
- Allow any source through firewall
- Control access with username/password in the web application
- Allow DEV team privileged server access

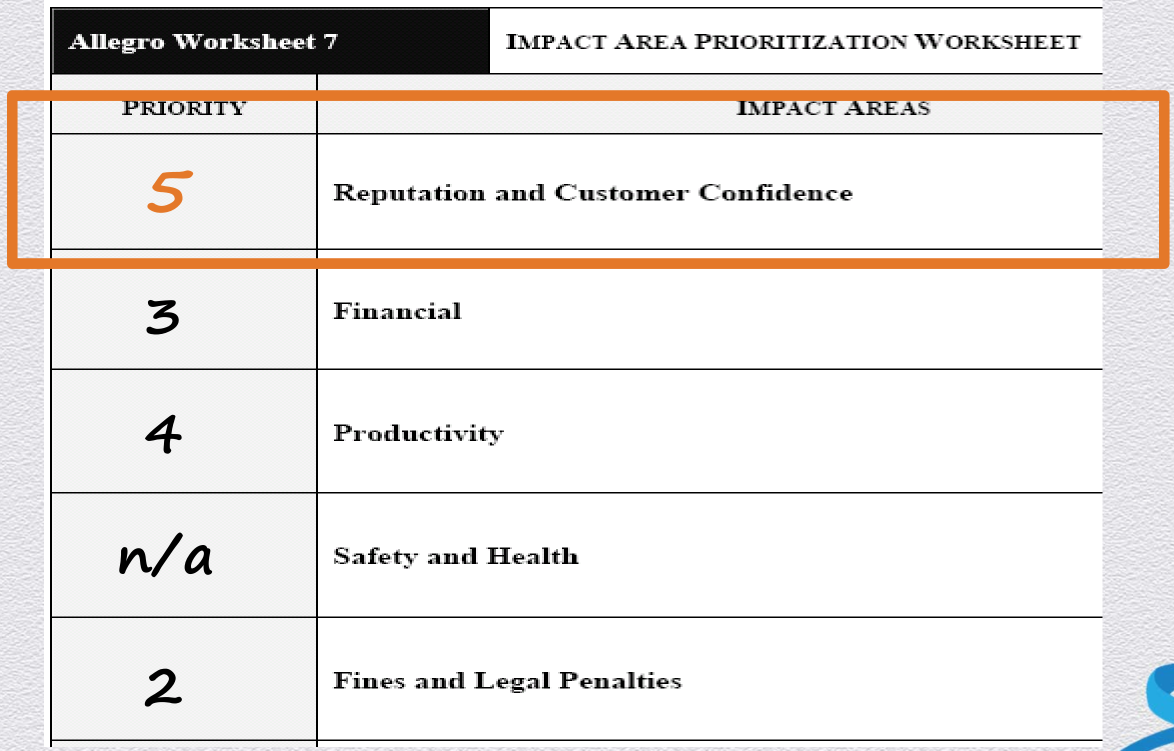


What is important to the organization?

- Financial
- Legal
- Reputational
- Regulatory

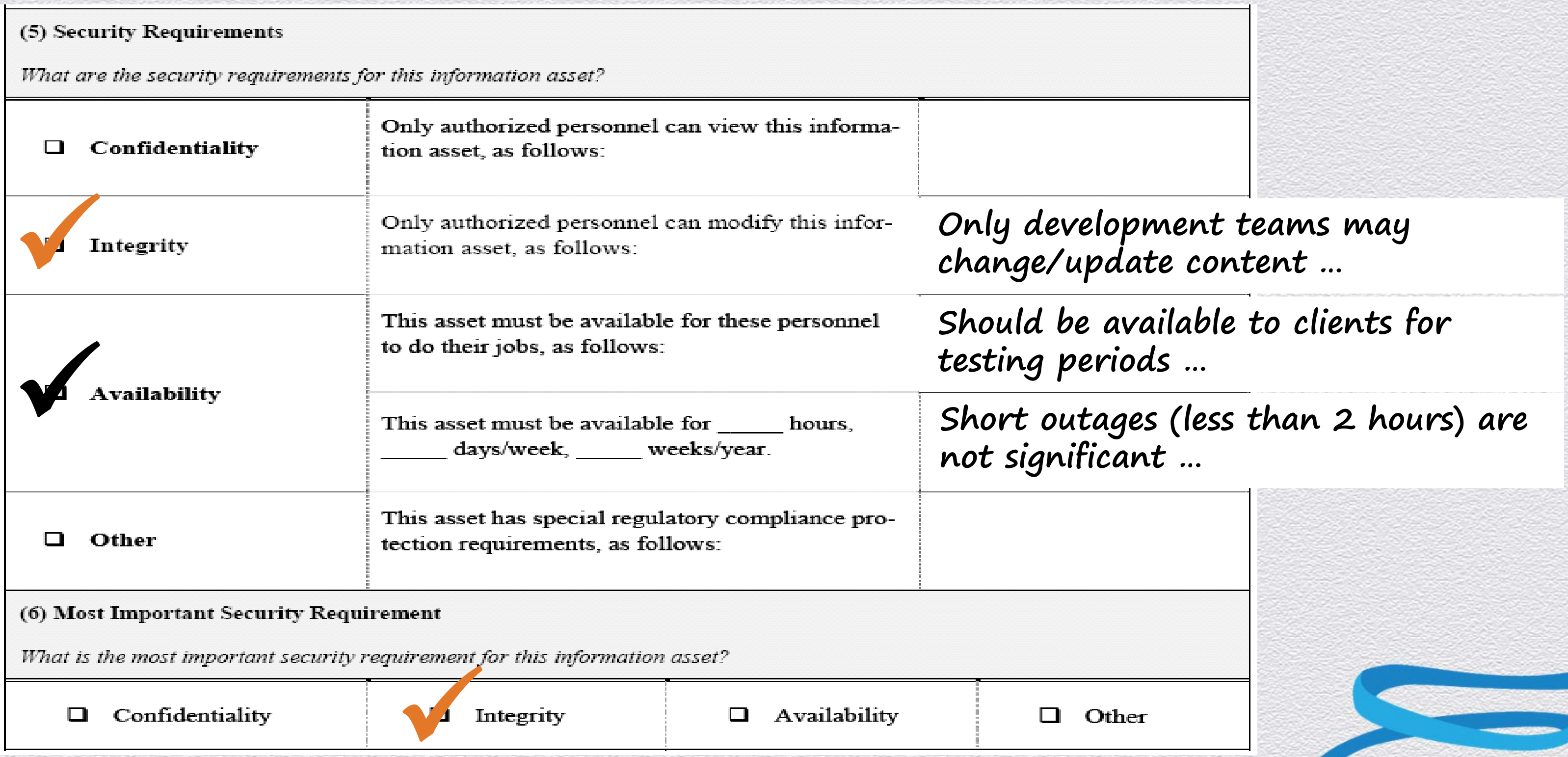
- Establish a risk profile
  - The Business Owner rates the resource’s importance to the organization
  - Should account for individual CIA(A) considerations
  - Can be completed even before any implementation decisions are made

AcmeHealth Prioritization using OCTAVE



Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	IMPACT AREAS
5	Reputation and Customer Confidence
3	Financial
4	Productivity
n/a	Safety and Health
2	Fines and Legal Penalties

AcmeHealth Security Requirements using OCTAVE



(5) Security Requirements

What are the security requirements for this information asset?

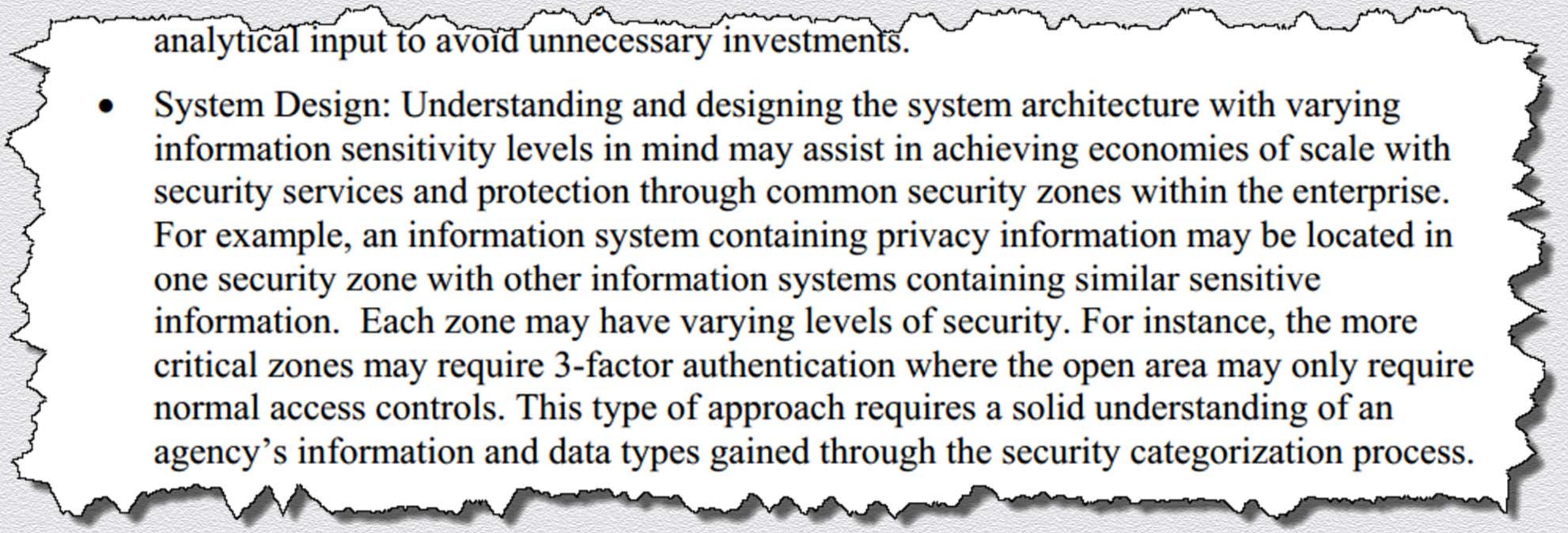
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	
✓ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Only development teams may change/update content …
✓ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Should be available to clients for testing periods …
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	Short outages (less than 2 hours) are not significant …
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

❑ Confidentiality	✓ Integrity	❑ Availability	❑ Other

How should this be used?



analytical input to avoid unnecessary investments.

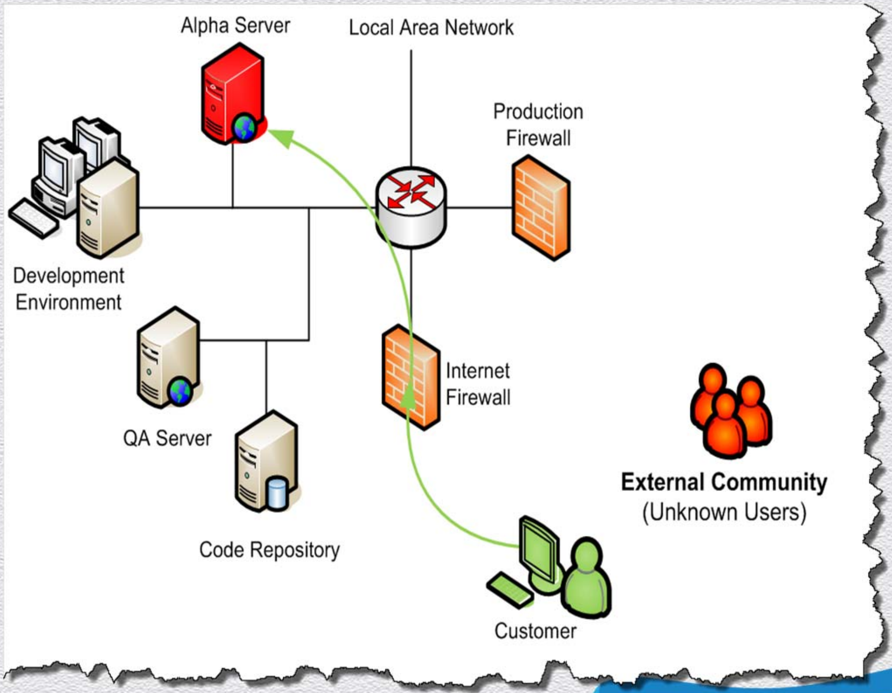
- System Design: Understanding and designing the system architecture with varying information sensitivity levels in mind may assist in achieving economies of scale with security services and protection through common security zones within the enterprise. For example, an information system containing privacy information may be located in one security zone with other information systems containing similar sensitive information. Each zone may have varying levels of security. For instance, the more critical zones may require 3-factor authentication where the open area may only require normal access controls. This type of approach requires a solid understanding of an agency's information and data types gained through the security categorization process.

NIST SP 800-60

Threats to AcmeHealth

Threat Surface

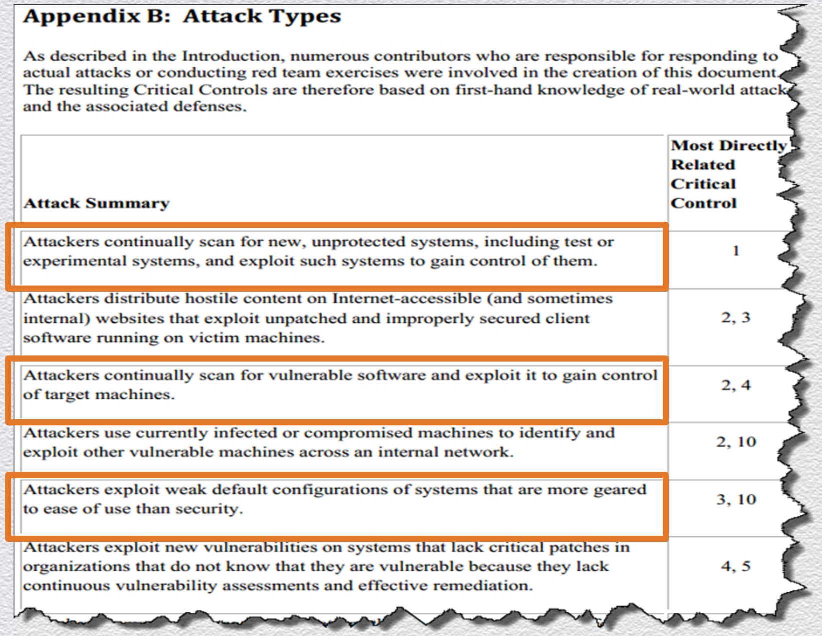
- Intended flow:
  - Customer access to web application on alpha server
- Unintended flows:
  - External unknown access to web application
  - External unknown access to web server



What are likely threats to AcmeHealth?

External Hacking results in Server Confidentiality & Integrity breaches

Common attack scenarios



Appendix B: Attack Types

As described in the Introduction, numerous contributors who are responsible for responding to actual attacks or conducting red team exercises were involved in the creation of this document. The resulting Critical Controls are therefore based on first-hand knowledge of real-world attack and the associated defenses.

Attack Summary	Most Directly Related Critical Control
Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them.	1
Attackers distribute hostile content on Internet-accessible (and sometimes internal) websites that exploit unpatched and improperly secured client software running on victim machines.	2, 3
Attackers continually scan for vulnerable software and exploit it to gain control of target machines.	2, 4
Attackers use currently infected or compromised machines to identify and exploit other vulnerable machines across an internal network.	2, 10
Attackers exploit weak default configurations of systems that are more geared to ease of use than security.	3, 10
Attackers exploit new vulnerabilities on systems that lack critical patches in organizations that do not know that they are vulnerable because they lack continuous vulnerability assessments and effective remediation.	4, 5

SANS Critical Controls for Effective Cyber Defense

Data breach thr s

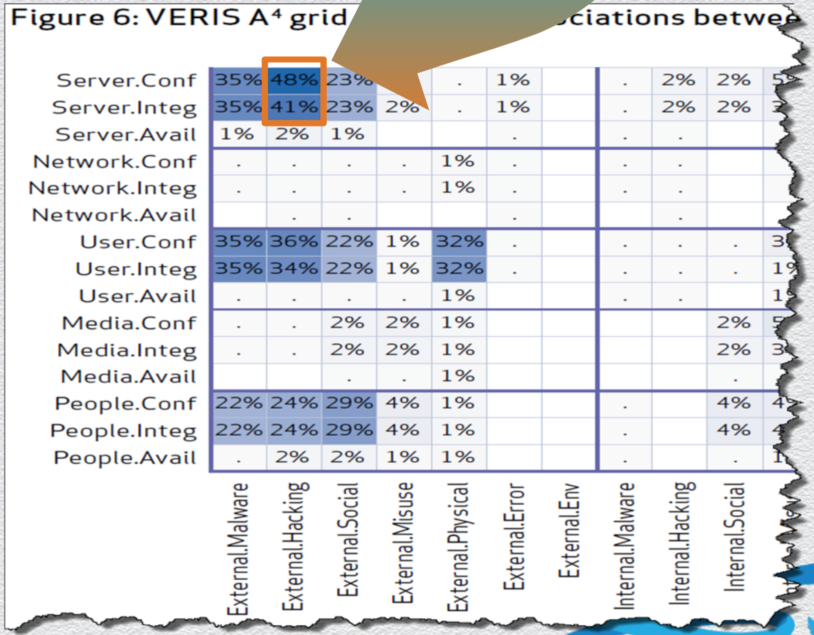


Figure 6: VERIS A^4 grid ciations betwee

	External.Malware	External.Hacking	External.Social	External.Misuse	External.Physical	External.Error	External.Env	Internal.Malware	Internal.Hacking	Internal.Social	
Server.Conf	35%	48%	23%		.	1%		.	2%	2%	5
Server.Integ	35%	41%	23%	2%	.	1%		.	2%	2%	3
Server.Avail	1%	2%	1%			.		.	.		
Network.Conf	.	.	.	.	1%	.		.	.		
Network.Integ	.	.	.	.	1%	.		.	.		
Network.Avail		.	.			.			.		
User.Conf	35%	36%	22%	1%	32%	.		.	.	.	3
User.Integ	35%	34%	22%	1%	32%	.		.	.	.	1
User.Avail	.	.	.	.	1%			.	.		1
Media.Conf	.	.	2%	2%	1%					2%	5
Media.Integ	.	.	2%	2%	1%					2%	3
Media.Avail			.	.	1%					.	
People.Conf	22%	24%	29%	4%	1%			.		4%	4
People.Integ	22%	24%	29%	4%	1%			.		4%	4
People.Avail	.	2%	2%	1%	1%			.		.	1

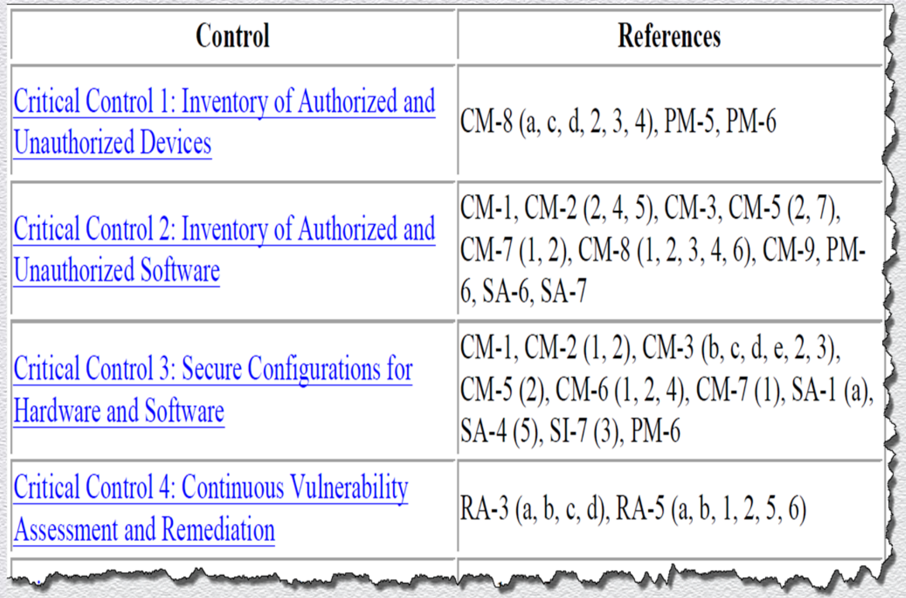
Verizon DBIR 2013

Control Selection

SANS Critical Controls

1. Inventory of Authorized and Unauthorized Devices and Software
2. Secure Configurations for Hardware and Software
3. Continuous Vulnerability Assessment and Remediation
4. Secure Configurations for Network Devices

NIST 800-53 Mapping



Control	References
Critical Control 1: Inventory of Authorized and Unauthorized Devices	CM-8 (a, c, d, 2, 3, 4), PM-5, PM-6
Critical Control 2: Inventory of Authorized and Unauthorized Software	CM-1, CM-2 (2, 4, 5), CM-3, CM-5 (2, 7), CM-7 (1, 2), CM-8 (1, 2, 3, 4, 6), CM-9, PM-6, SA-6, SA-7
Critical Control 3: Secure Configurations for Hardware and Software	CM-1, CM-2 (1, 2), CM-3 (b, c, d, e, 2, 3), CM-5 (2), CM-6 (1, 2, 4), CM-7 (1), SA-1 (a), SA-4 (5), SI-7 (3), PM-6
Critical Control 4: Continuous Vulnerability Assessment and Remediation	RA-3 (a, b, c, d), RA-5 (a, b, 1, 2, 5, 6)

SANS Critical Controls for Effective Cyber Defense

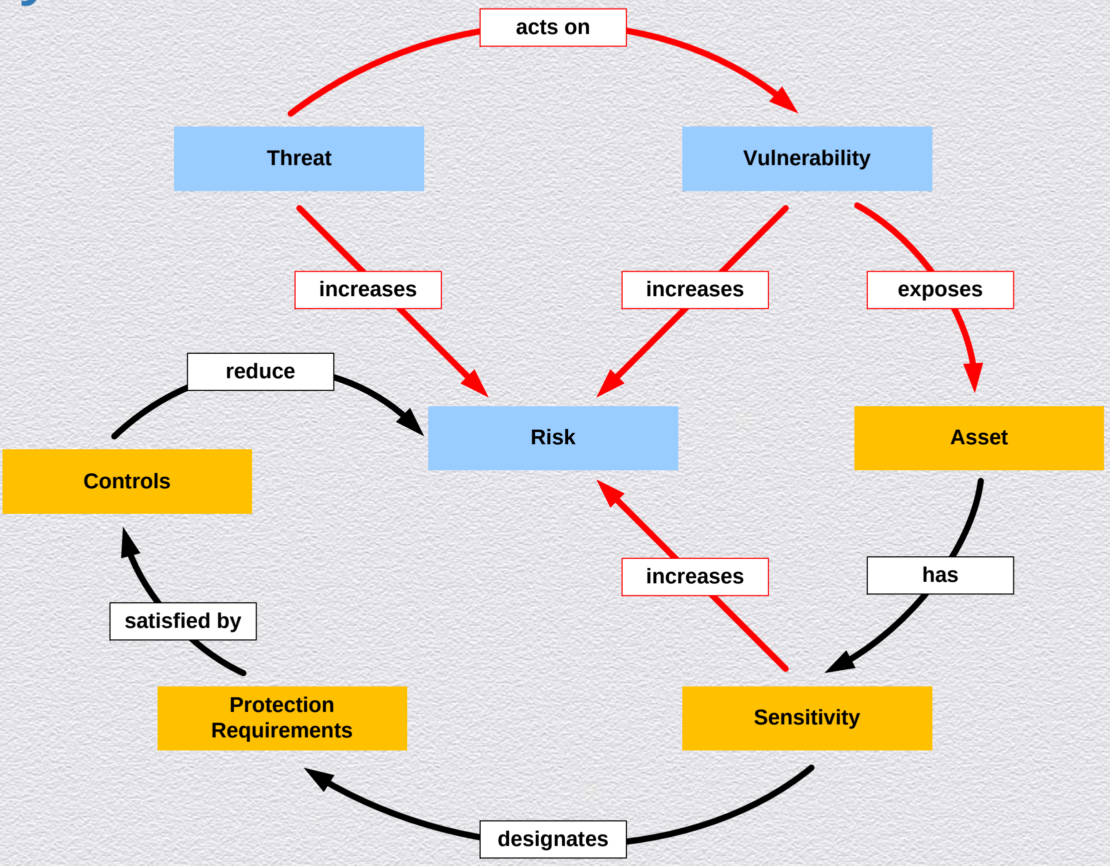
RSACONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Information Flows

A Different Approach

- Information Flow based
- Risk focused
- Provides structure for determining:
  - Control requirements per flow
  - Placement of physical, logical, and virtual boundaries
  - Placement of resources
- Generates reusable patterns

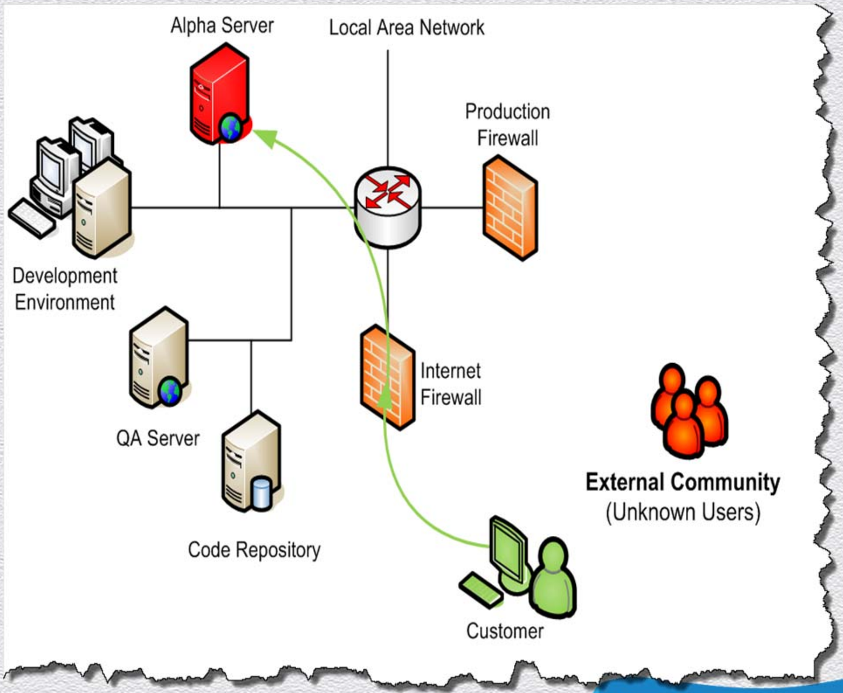
Risk Ecosystem



What is our exposure and how do we reduce it?

Risk Reduction Approaches

1. Reduce the Threat Surface
2. Mitigate Vulnerabilities
3. Reduce the Sensitivity of Resources



Reduce Threat Surface

Information Flow	Threat Surface	Vulnerability (CVSS)	Sensitivity	Exposure
Any -> Alpha Server	Large anonymous 5	SQL Injection 10	High 4	**200**

Threat Surface:

5 - large anonymous population (any Internet host)

4 - extended corporate population (employees & vendors)

3 - limited and known population (employees & clients)

2 - general corporate population (employees)

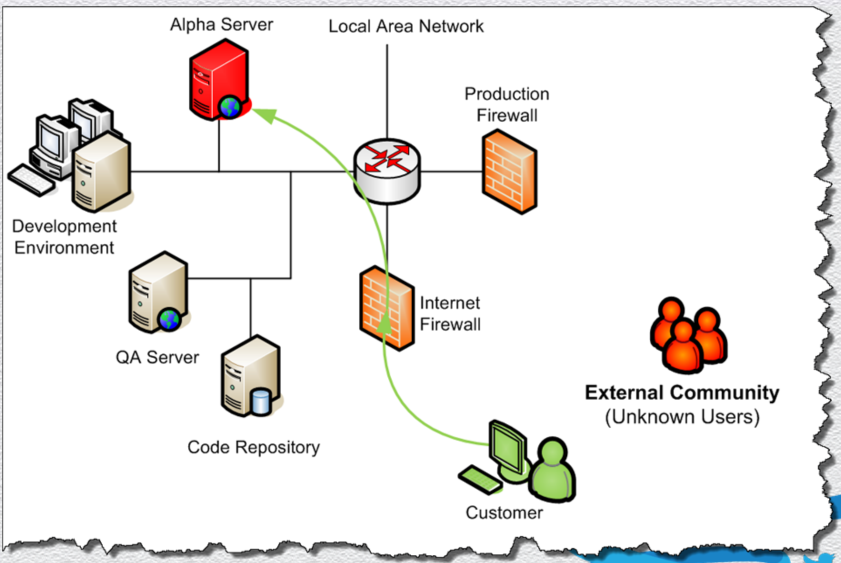
1 - small and trusted population (resource administrators)

Risk Sensitivity:

4 - compromise would be severe or catastrophic

3 - compromise would be significant or serious

2 - compromise would be minor or limited



Classifying Information Flows

Trustworthiness

- internal
- external
- ----
- trusted
- untrusted

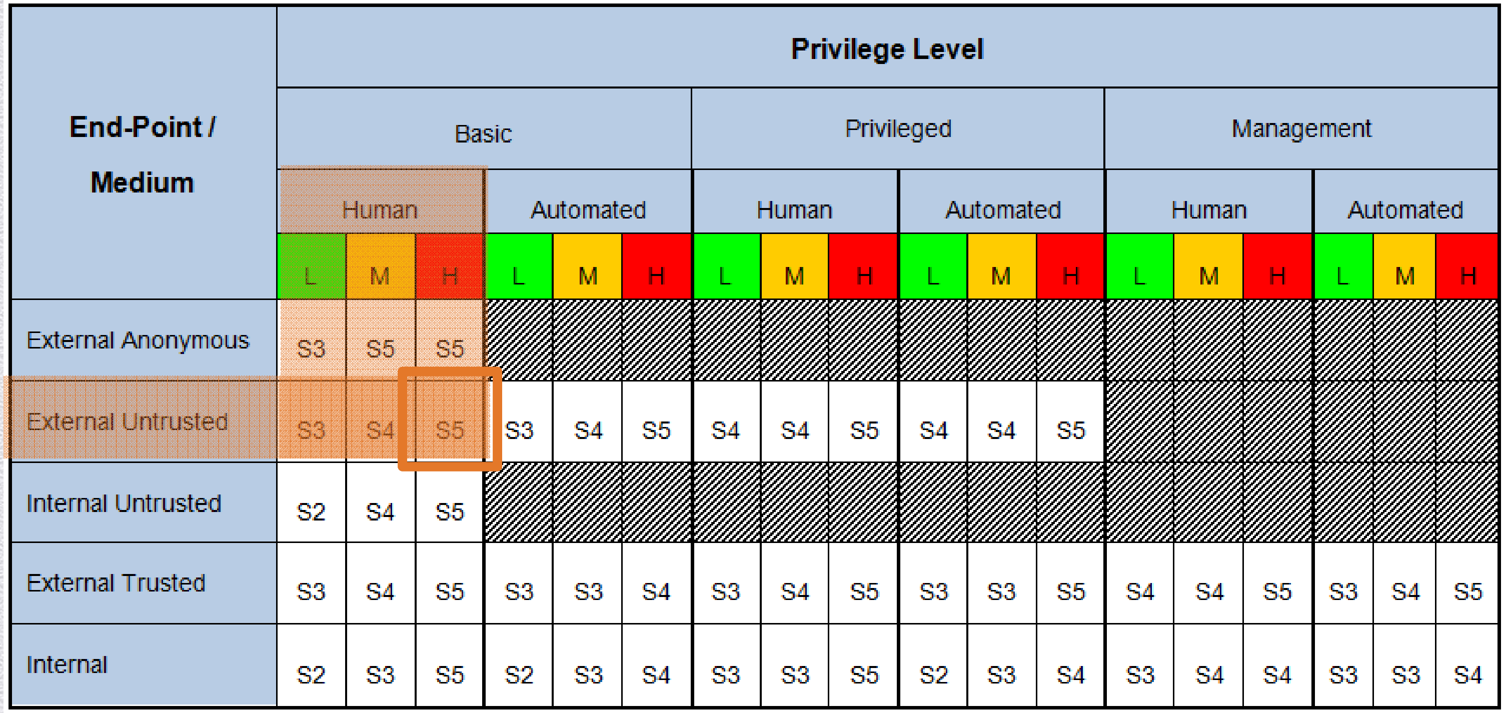
Flow initiator

- human
- automated

Privilege level

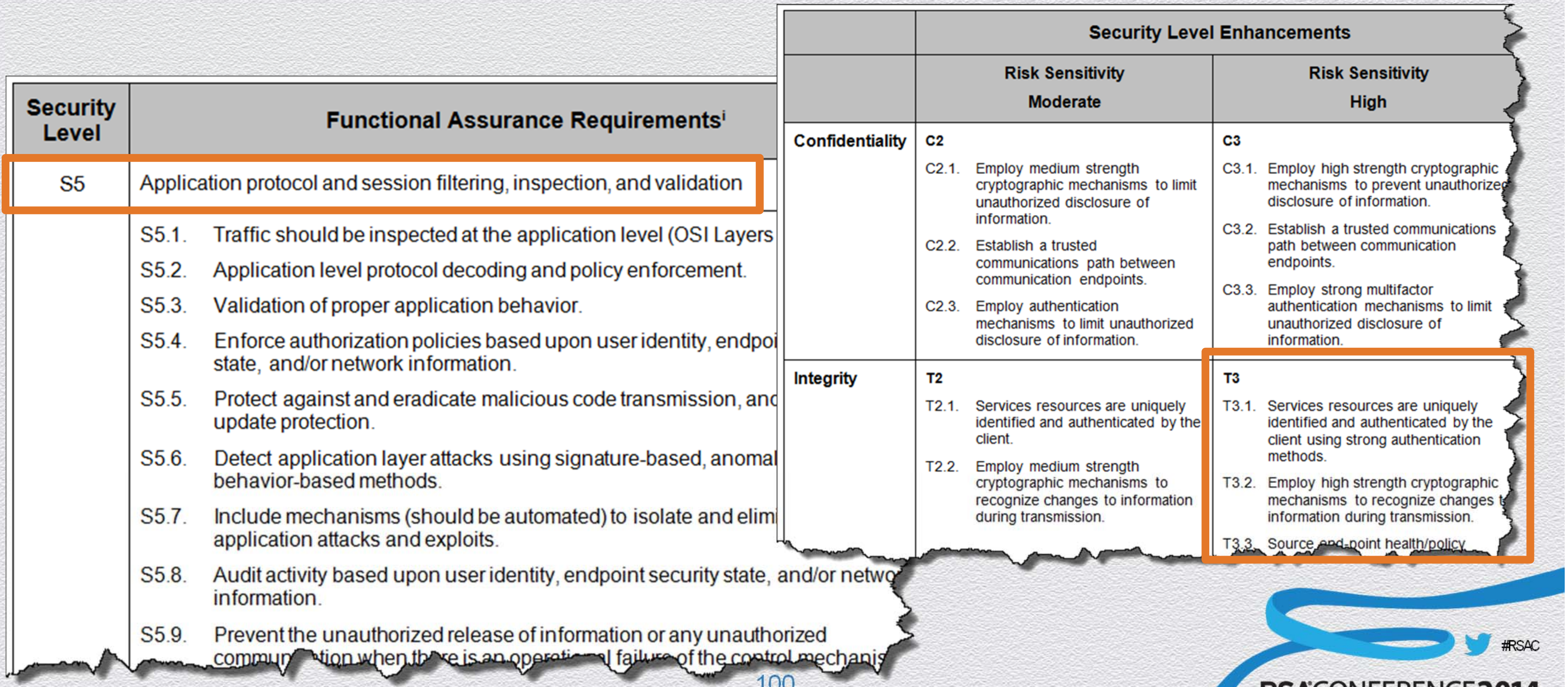
- basic
- privileged
- management

Mapping Flows to Security Requirements



End-Point / Medium	Privilege Level																	
	Basic						Privileged						Management					
	Human			Automated			Human			Automated			Human			Automated		
	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
External Anonymous	S3	S5	S5	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
External Untrusted	S3	S4	S5	S3	S4	S5	S4	S4	S5	S4	S4	S5	▨	▨	▨	▨	▨	▨
Internal Untrusted	S2	S4	S5	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
External Trusted	S3	S4	S5	S3	S3	S4	S3	S4	S5	S3	S3	S5	S4	S4	S5	S3	S4	S5
Internal	S2	S3	S5	S2	S3	S4	S3	S3	S5	S2	S3	S4	S3	S4	S4	S3	S3	S4

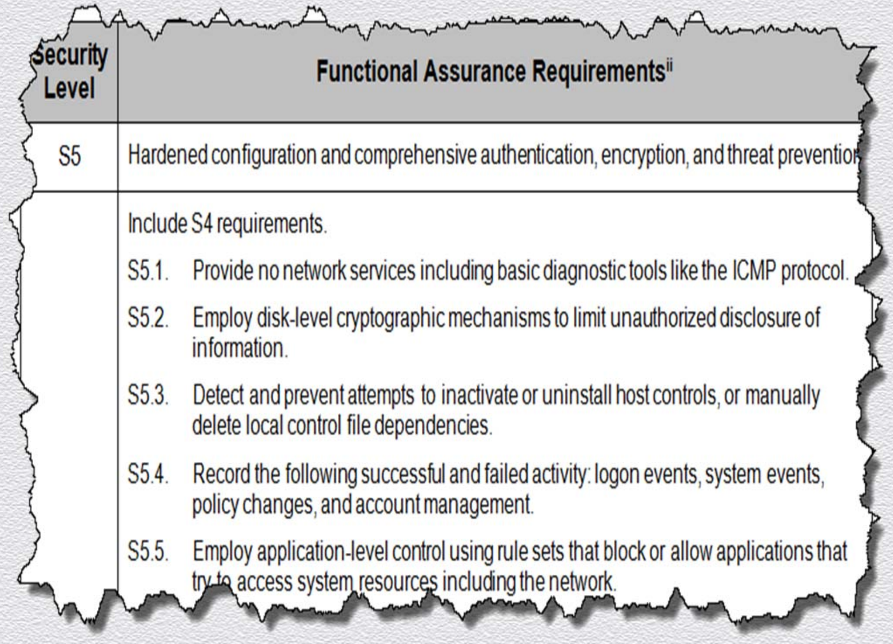
Defining Security Levels

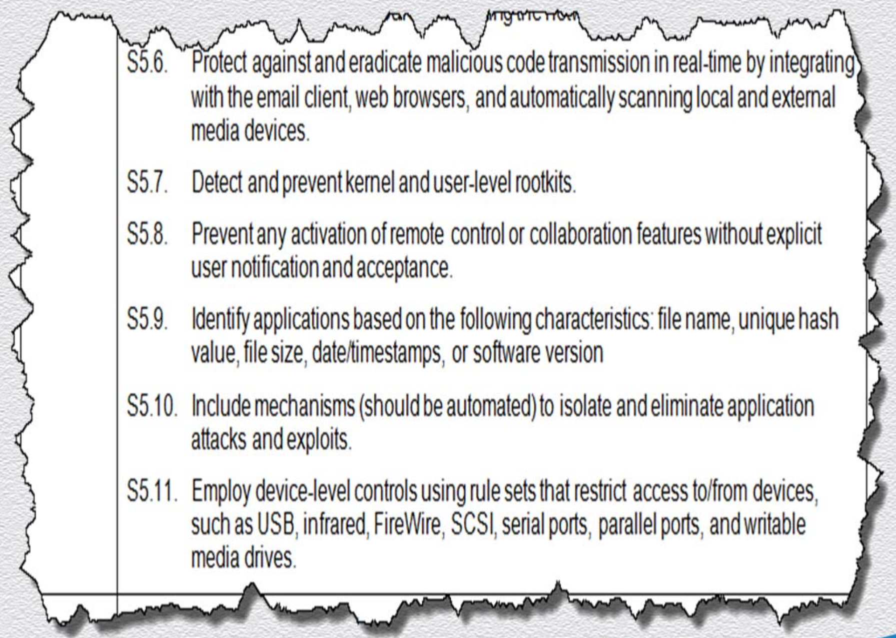


Security Level	Functional Assurance Requirements[i]
S5	Application protocol and session filtering, inspection, and validation
	S5.1. Traffic should be inspected at the application level (OSI Layers S5.2. Application level protocol decoding and policy enforcement. S5.3. Validation of proper application behavior. S5.4. Enforce authorization policies based upon user identity, endpoi state, and/or network information. S5.5. Protect against and eradicate malicious code transmission, and update protection. S5.6. Detect application layer attacks using signature-based, anomal behavior-based methods. S5.7. Include mechanisms (should be automated) to isolate and elim application attacks and exploits. S5.8. Audit activity based upon user identity, endpoint security state, and/or netwo information. S5.9. Prevent the unauthorized release of information or any unauthorized communication when there is an operational failure of the control mechanis

	Security Level Enhancements	
	Risk Sensitivity Moderate	Risk Sensitivity High
Confidentiality	C2 C2.1. Employ medium strength cryptographic mechanisms to limit unauthorized disclosure of information. C2.2. Establish a trusted communications path between communication endpoints. C2.3. Employ authentication mechanisms to limit unauthorized disclosure of information.	C3 C3.1. Employ high strength cryptographic mechanisms to prevent unauthorized disclosure of information. C3.2. Establish a trusted communications path between communication endpoints. C3.3. Employ strong multifactor authentication mechanisms to limit unauthorized disclosure of information.
Integrity	T2 T2.1. Services resources are uniquely identified and authenticated by the client. T2.2. Employ medium strength cryptographic mechanisms to recognize changes to information during transmission.	T3 T3.1. Services resources are uniquely identified and authenticated by the client using strong authentication methods. T3.2. Employ high strength cryptographic mechanisms to recognize changes t information during transmission. T3.3. Source end-point health/policy

End-Point Example



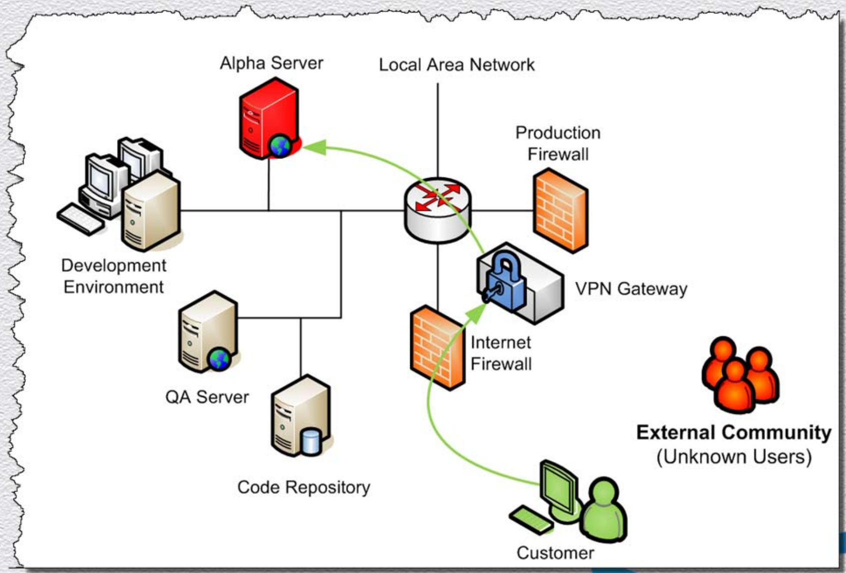


Security Level	Functional Assurance Requirements[ii]
S5	Hardened configuration and comprehensive authentication, encryption, and threat preventio
	Include S4 requirements. S5.1. Provide no network services including basic diagnostic tools like the ICMP protocol. S5.2. Employ disk-level cryptographic mechanisms to limit unauthorized disclosure of information. S5.3. Detect and prevent attempts to inactivate or uninstall host controls, or manually delete local control file dependencies. S5.4. Record the following successful and failed activity: logon events, system events, policy changes, and account management. S5.5. Employ application-level control using rule sets that block or allow applications that try to access system resources including the network. S5.6. Protect against and eradicate malicious code transmission in real-time by integrating with the email client, web browsers, and automatically scanning local and external media devices. S5.7. Detect and prevent kernel and user-level rootkits. S5.8. Prevent any activation of remote control or collaboration features without explicit user notification and acceptance. S5.9. Identify applications based on the following characteristics: file name, unique hash value, file size, date/timestamps, or software version S5.10. Include mechanisms (should be automated) to isolate and eliminate application attacks and exploits. S5.11. Employ device-level controls using rule sets that restrict access to/from devices, such as USB, infrared, FireWire, SCSI, serial ports, parallel ports, and writable media drives.

Proposed Solution

Information Flow	Threat Surface	Vulnerability (CVSS)	Sensitivity	Exposure
Clients -> VPN Gateway VPN -> Alpha Server	limited and known 3	SQL Injection 10	High 4	~~200~~ 120

- A traditional firewall doesn't meet these requirements on its own
- Restricting firewall to client networks may not be manageable
- Application may be lacking authentication
- What is the risk appetite or tolerance?



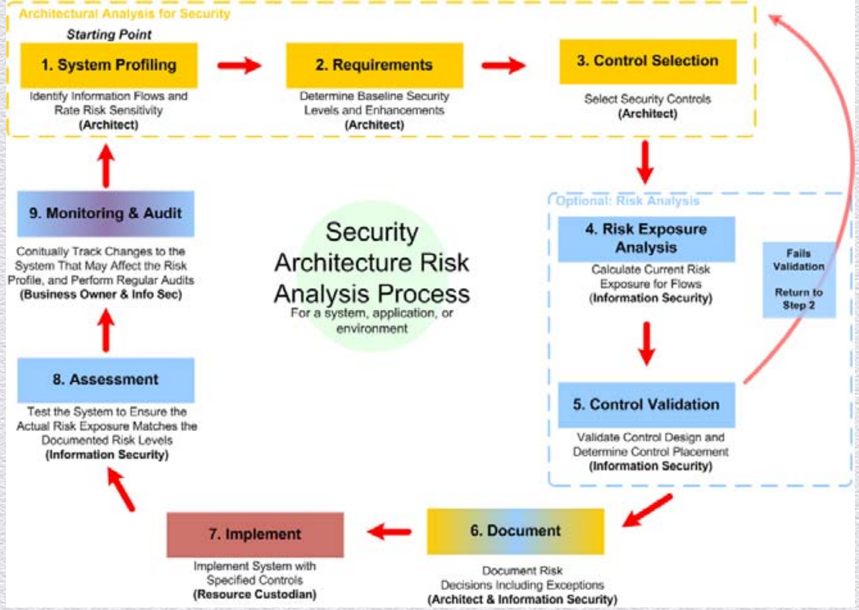
Additional Risk Scenarios

- Transitive risk to other systems on the internal network?
- How will the Alpha get Internet access for updates, patching, etc.?
- How do you ensure sensitive data isn’t used in Alpha?
- How would the security requirements be different if the risk profile of the resource or trust relationship were different?

Repeatable Process

Analysis Process Approaches

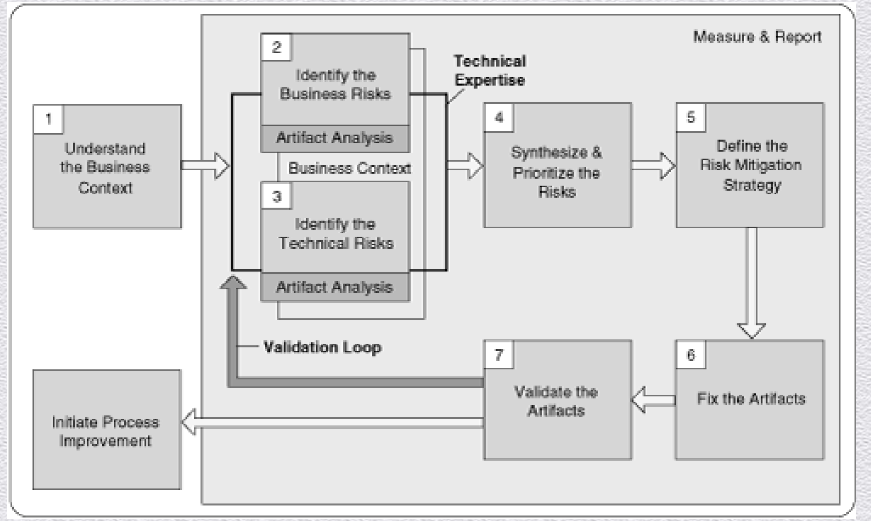
Allows for approved patterns



Architectural Analysis for Security
Starting Point
1. System Profiling
Identify Information Flows and Rate Risk Sensitivity (Architect)
2. Requirements
Determine Baseline Security Levels and Enhancements (Architect)
3. Control Selection
Select Security Controls (Architect)
Optional: Risk Analysis
4. Risk Exposure Analysis
Calculate Current Risk Exposure for Flows (Information Security)
Fails Validation
Return to Step 2
5. Control Validation
Validate Control Design and Determine Control Placement (Information Security)
6. Document
Document Risk Decisions Including Exceptions (Architect & Information Security)
7. Implement
Implement System with Specified Controls (Resource Custodian)
8. Assessment
Test the System to Ensure the Actual Risk Exposure Matches the Documented Risk Levels (Information Security)
9. Monitoring & Audit
Conitually Track Changes to the System That May Affect the Risk Profile, and Perform Regular Audits (Business Owner & Info Sec)
Security Architecture Risk Analysis Process
For a system, application, or environment

http://www.ossie-group.org/publications.html

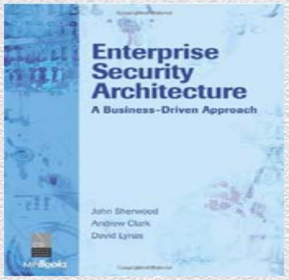
Cigital flow fits into RMF



Measure & Report
1
Understand the Business Context
2
Identify the Business Risks
Artifact Analysis
Technical Expertise
Business Context
3
Identify the Technical Risks
Artifact Analysis
4
Synthesize & Prioritize the Risks
5
Define the Risk Mitigation Strategy
Validation Loop
7
Validate the Artifacts
6
Fix the Artifacts
Initiate Process Improvement

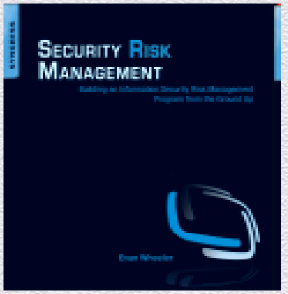
http://www.informit.com/articles/article.aspx?p=446451

Reference Materials



Enterprise Security Architecture: A Business-Driven Approach

- ISBN: 978-1578203185
- Publisher: CRC Press
- Publication Date: November 2005
- Amazon Link: http://amzn.com/157820318X


Security Risk Management
Building an Information Security Risk Management Program from the Ground Up
Evan Wheeler

Security Risk Management: Building an Information Security Risk Management Program from the Ground Up

- ISBN: 978-1597496155
- Publisher: Syngress
- Publication Date: May 2011
- Amazon Link: http://amzn.to/hyrMvC

Security Patterns Repository: http://www.scrypt.net/~celer/securitypatterns/

SANS Critical Controls for Effective Cyber Defense

Verizon Data Breach Investigations Report 2013