RE-THINKING RMF

KURT DANIS, CISSP-ISSEP
SECRETARY, ISSA, COLORADO SPRINGS CHAPTER
SEPTEMBER 2023

This presentation derived from a concept paper, “RMF for leadership”.

This presentation addresses concepts for RMF practitioners; and explores the “so-what” factors for those in the throes of the RMF pipeline.

This brief will provide characterizations, principles, and lessons-learned from my RMF experience.

The presentation title comes from Adam Grant’s book “Think Again”.

History

Rainbow Series	DITSCAP	DIACAP	RMF
Computer Security	Network Security	Netcentric Security	Mission Assurance

Assertion: **Risk Management should not focus on dealing with problems; it should focus on preventing them**. Looking at Risks from every domain and process in the service lifecycle, capturing them and planning for them, will help the organization manage risk effectively, reducing negative impact, uncertainty and costs, and conversely exploiting positive impact. – DoD Enterprise Service Management Framework (DESMF), Edition 3, 04Mar2016

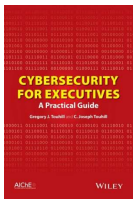
2

- RMF seeks a mission assurance (MA) balance with the **security posture** requirements*
- RMF serves as a common methodology for the DoD, IC, and civil agencies (**as a result, RMF is standardized RM approach, and uses a common taxonomy**)
- RMF quantifies and documents system threat sources (e.g. supply chain risk management, espionage, insider threat, threats against critical technology/critical information, etc.)
- RMF links and communicates **risk to the stakeholders** (i.e. mission owners, mission supporters, system developers, system/asset owners, project managers, other Organizations, the Nation, etc.) ➔ **RMF not a just vulnerability checklist**
- RMF stakeholders extend beyond the tactical level: DoD CIO, Risk Executive Function, RMF TAG, Mission area owners, Acquisition, DISA, Component CIOs,…

* Reference: DOD Directive 3020.40, Mission Assurance (MA), published November 29, 2016: "In addition to the responsibilities in Paragraph 2.8., the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense: a. Provides guidance to the DoD Components for submitting and displaying MA-related resource requirements for risk management **within budget submissions**."

C&A Transformation Goals

1. Define a ***common set of trust (impact) levels*** and adopt and apply them across the Intelligence Community (IC) and DoD. Organizations will no longer use different levels with different names based on different criteria.
2. Adopt ***reciprocity*** as the norm, enabling organizations to accept the approvals by others without retesting or reviewing.
3. Define, document, and adopt ***common security controls***, using NIST Special Publication (SP) 800-53 as a baseline.
4. Adopt a ***common lexicon***, using CNSS Instruction 4009 as a baseline thereby providing DoD and IC a common language and common understanding.
5. Institute a ***senior risk executive function***, which bases decisions on ***an "enterprise" view of risk considering all factors***, including mission, IT, budget, and security.
6. Incorporate information assurance (IA) into ***Enterprise Architectures*** and deliver IA as ***common enterprise services*** across the IC and DoD.
7. Enable a ***common process*** that incorporates security within the ***"lifecycle"*** processes and eliminate security-specific processes. The common process will be adaptable to various development environments.



3

RMF originated as a "C&A Transformation" project in 2007. Seven foundational goals are shown here.

In general, [**cybersecurity] "…is a <u>multidisciplinary approach</u> to managing risk**; a principle concern of executives."

--- Cybersecurity for Executives – A Practical Guide, by father (Joseph) and son Greg Touhill.

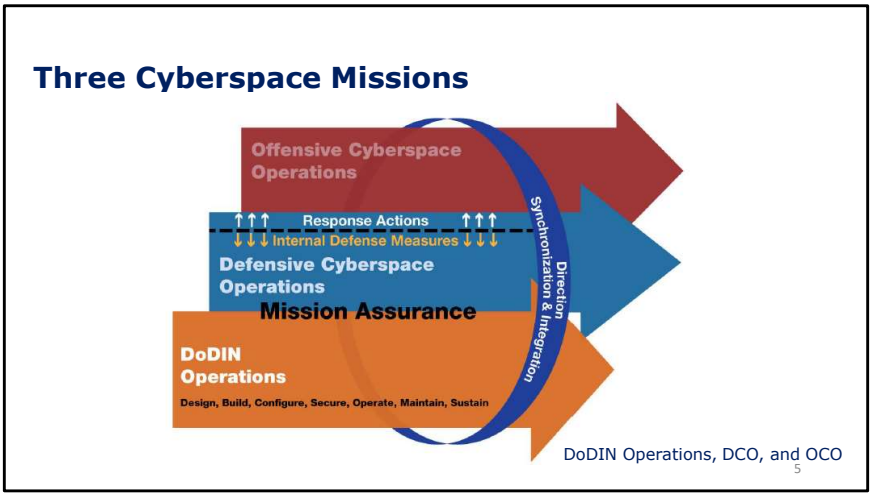
Greg Touhill once served as the Federal Chief Information Security Officer. Greg is a CISSP and CISM

RMF: a culmination of many objectives

4

RMF is a like a collage of activities that embody many objectives, ideals of the past, and addresses new tenets never before handled in a systematic way.

Word collage developed by Kurt Danis using an online tool called Word Cloud. http://www.wordclouds.com/



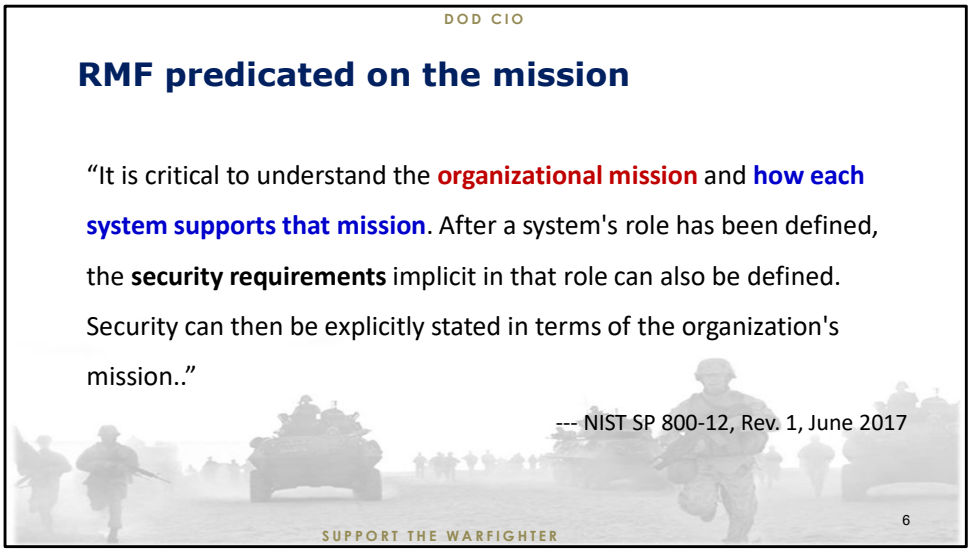
Joint Publication 3-12, Cyberspace Operations, defines the three missions of Cyberspace Operations for the Department of Defense (DoD) as DoD Information Network (DoDIN) Operations, Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO), which are illustrated in in this figure.

Based on the definitions, RMF clearly resides within DODIN set of Operations.

Reference: Army Chief Information Officer/G6, (2015).
Army Network Campaign Plan 2020 & Beyond.
Retrieved from
http://ciog6.army.mil/Portals/1/ANCP/ANCP%20PRINT%206%20FEB%2015.pdf, 1February 2016

Three Cyberspace Missions (Source: Joint Pub. 3-12, 8 June 2018):

- Department of Defense information network (DODIN): Operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and **preserve the confidentiality, availability, and integrity** of the Department of Defense information network. Also called DODIN operations.
- Offensive Cyber Operations (OCO): Missions intended to project power in and through cyberspace.
- Defensive Cyber Operations (DCO): Now called defensive cyberspace operations-response actions. Operations that are part of a defensive cyberspace operations mission that are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system. Also called DCO-RA.



To begin with, the Mission is about our nation (people).

In cybersecurity terms, it's all about the information (as opposed to protecting the system).

Information Security: Defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

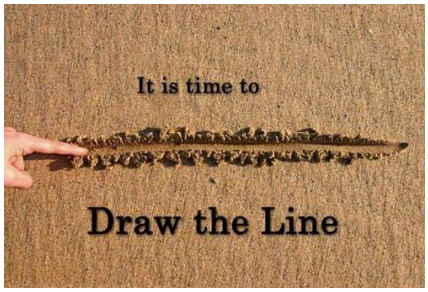
Sometimes, going back to the basics makes a difference on the Level of Effort necessary for protecting the "information". An untrusted system for example should imply that the resident information is NOT worth protecting.

Recent policy is predicated on Trusted Systems. A reasonable interpretation of the DoDIN definition (Joint Publication 1-02**) would say trusted systems require Defense-in-Depth cyber security measures. At a higher level, FISMA of 2014 reinforces all our current policies for trusted systems.** For example, CJCSI 6510.01F is predicated on TRUSTED systems leading to connections to other TRUSTED systems. The following cyber security measures state DOD ISs (i.e. trusted systems) shall be engineered to:
(1) Implement a defense-in-depth strategy for ISs and supporting infrastructures through an incremental process of protecting critical assets or data first. The defense-in-depth strategy must establish protection and trust across various network layers (e.g., application, presentation, session, transport, network, data link, or physical) IAW DODD 8500.01E (reference a).
(2) Ensure network and infrastructure services provide confidentiality, availability, integrity, authentication, and non-repudiation.
(3) Defend the perimeters of enclaves by establishing a well-defined boundary with protection mechanisms (e.g., firewalls, CDSs, DMZs, ACLs, IDSs, and IPSs).

TRUSTED SYSTEM DEFINED. Older concepts come from older policies; and while obsolete, they still have profound meaning and utility today. Bullets below help define a "Trusted System". Ref: Red Book (NCSC-TG-005, Version 1) 31Jul1987

- A trusted network is able to control both the reading and writing of shared sensitive information.
- The policy enforcement by trusted components in a "single trusted system" exhibits a common level of trust throughout.
- A "single trusted system" network implements a reference monitor to enforce the access of subjects to objects in accordance with an explicit and well-defined network security policy.
- Every component that is trusted must enforce a component-level security policy that may contain elements of the overall network security policy. The sum of all component-level security policies must be shown to enforce the overall network security policy.

Risk Management Steps



Step 1: Risk **F**raming
Step 2: Risk **A**ssessment
Step 3: Risk **R**esponse
Step 4: Risk **M**onitoring

Ref: Appendix E, NIST Special Publication 800-39

"Take calculated risks. That is quite different from being rash." -- General George S. Patton (1885-1945)

Need to be decisive; not passive (i.e. "I'll take your word for it"). Leadership must draw the line.

Risk Framing (Step 1 for example) is a decisive action that involves:

- Identifying assumptions that affect how risk is assessed, responded to, and monitored within the organization.
- Identifying constraints on the conduct of risk assessment, risk response, and risk monitoring activities within the organization.
- Identifying the level of risk tolerance for the organization.
- Identifying priorities and trade-offs considered by the organization in managing risk.

Risk Assessment (Step 2) another assertive action that involves:

- Identifying threats to and vulnerabilities in organizational information systems and the environments in which the systems operate.
- Determining risk to organizational operations and assets, individuals, other organizations, and the Nation if identified threats exploit identified vulnerabilities.

Risk Response (Step 3) involves:

- Identifying alternative courses of action to respond to risk determined during the risk assessment.
- Evaluating alternative courses of action for responding to risk.
- Deciding on the appropriate course of action for responding to risk.
- Implementing the course of action selected to respond to risk.

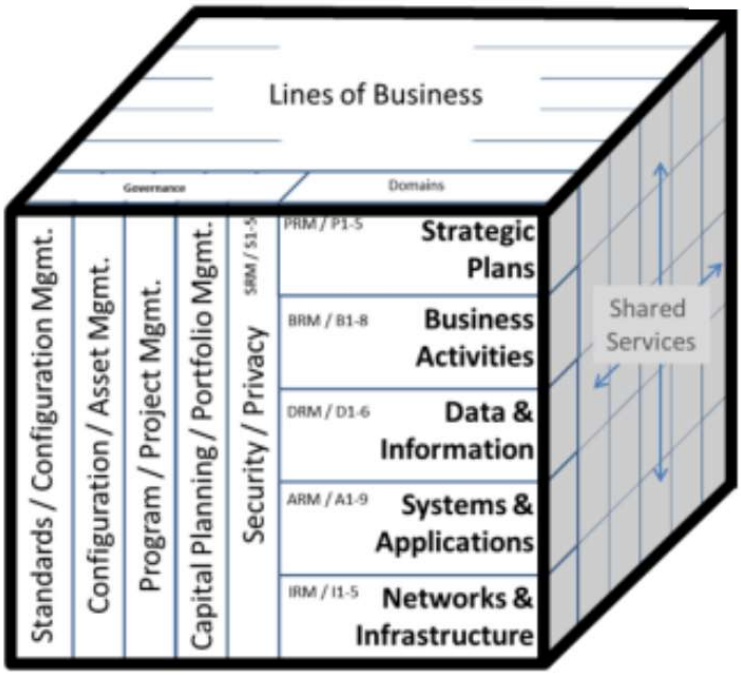
Risk Monitoring (Step 4) involves:

- Developing a risk monitoring strategy for the organization that includes the purpose, type, and frequency of monitoring activities.
- Monitoring organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.

--- Appendix E, NIST Special Publication 800-39

Next, we're going to talk about Architecture.

Data Feeds
Mission Apps
Infrastructure



8

So, I got a chance to study the science of enterprise architecture.

This benign image came from a FEAF document. "Federal Enterprise Architecture Framework", or FEAF, Version 2, dated January 29, 2013.

The domains included Strategic Plans, Business Activities, Data, Systems and Applications, and Infrastructures. Blah, blah, blah.

Wait a minute! The RMF community thrives on systems defined by Data Feeds, Mission Apps, and Infrastructures.

Remember that. It's a reoccurring theme for every system: Data Feeds, Mission Apps, and Infrastructures

Architecture

Eero Saarinen, 1910 – 1961

- American architectural design during the 1950s

- Architecture means the ruling art

9

OK, let's talk really about architecture. The next slide dives into policy not so graphic. There are no pretty pictures, so this slide makes up for it.

Architectural is about a theme.

Who knows where this image comes from? [Terminal 5 at New York's John F. Kennedy Airport. The building now serves as the TWA Hotel, $500 - $1,000 per day]

The famous Finnish architect, Eero Saarinen recommends this design principle (architecture):
"Always design a thing by considering it in its next larger context--- a chair in a room, a room in a house, a house in an environment, an environment in a city."

An architecture, loosely defined, is the structure of components and their relationships. When architecture is applied to enterprise, we get enterprise architecture -- the structure of components in an enterprise and their relationships.

In a publication called, Imprimis, I captured this statement, "Aristotle writes that the architect does not know how to lay bricks as well as the bricklayer, but he knows how to direct the bricklayer toward the completion of the building. The word "architect" comes from two Greek words: arche, which means "ruling principle," and techne, which means "art" or "making" (the word "technology" derives from this word as well). **So, architecture means the ruling art,** and it is a form of the kind of understanding every person must have to manage his life. The classical word for it is prudence. It is the common-sense capacity we each have to pursue the proper ends of life amidst a welter of constantly shifting circumstances."

Dr. Larry Arnn, Imprimis, March/April 2020, Volume 49, Number 3/4

DoD Cyber Discipline (2015)

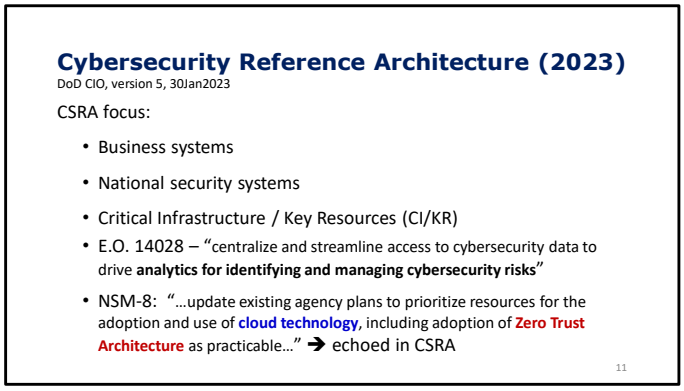
Four lines of Effort:

- 1. Ensuring Strong Authentication – How do users log onto devices and systems?
- 2. Hardening Devices – Are devices properly configured and regularly updated?
- 3. Reducing the Attack Surface – How many things directly connect to the public Internet?
- 4. Detecting and Responding to Potential Intrusions – Can cyber defenders do their jobs?

10

OK, let's go back in time for cybersecurity. Remember the 2015 DoD Cyber Discipline?

The architectural theme was 4 Lines of Effort. You may remember this; or you might remember another thematic set cyber principles.



Now, let's go forward in time... Let's talk about the future.

CSRA is the Guide to modernize cybersecurity. Version 5 of the CSRA advances DoD's defense business systems, national security systems, and critical infrastructure / key resources through an evolution to integrate ZT principles.

The CSRA is underpinned by EO 14028 and NSM-8.

In 2021, Executive Order 14028 directed the Federal Government to "make bold changes and significant investments" and use zero trust (ZT) to modernize cybersecurity. Section 3 of E.O. 14028, another presidential directive, is titled, "Improving the Nation's Cybersecurity"

Section 1 of **National Security Memorandum 8 (NSM-8),** *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* --- **to modernize cybersecurity through adoption of ZT architecture (ZTA). [Think NIST SP 800-207]**

> **NSM-8: "**Within 60 days of the date of this memorandum, **the head of each executive department or agency (agency) that owns or operates an NSS shall,** consistent with its statutory authority:
>
> (A) **update existing agency plans to** prioritize resources for the adoption and use of **cloud technology, including adoption of Zero Trust Architecture** as practicable;

The NSM authorizes the National Security Agency, through its role as National Manager for National Security Systems, to create Binding Operational Directives requiring agencies to take specific actions against known or suspected cybersecurity threats and vulnerabilities.

CSRA: "As organizations adopt ZTA, requirements and acquisition documents will need to define both the cybersecurity and cyber resilience threshold performance requirements to ensure they are contractually binding, measurable and testable." **So, if you write contracts, be ready to make ZTA Specific, Measurable, Achievable, Relevant, and Time-Bound.**

Review

12

SUMMARY

- We talked about the history or evolution of cyber risk management
- We know the C&A transformation started out in 2007 as a combined effort between IC, NIST, and DoD
- We know RMF is a cornucopia of activities (a multi-disciplinary effort)
- We know a little about the three missions of Cyberspace Operations; and that RMF is strictly part of the DoDIN
- We employ RMF for Mission Assurance
- We (the AO) must be decisive; not passive
- We talked about architecture; and it can imply a certain theme, or set the tone as a “ruling art”
- We quickly reviewed the 2015 DoD Cyber Discipline
- We then reviewed the 2023 Cybersecurity Reference Architecture (CSRA)

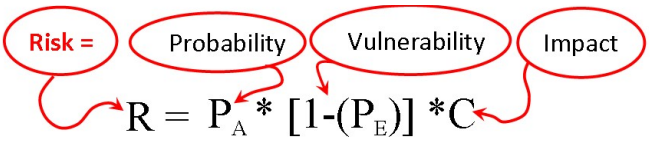
Linear vs. Exponential Heat Maps

13

The next few slides addresses a splinter topic.

Let's take a moment to re-think the Risk Matrix for cybersecurity. The risk matrix was borrowed from the acquisition community. The risk matrix also accounted for three risk factors: cost, schedule, and performance.

Qualitative Risk



- R = Risk to the facility of an adversary gaining access to assets (ranges from 0 to 1.0)
- P_A = Probability of an adversary attack during a period of time
- P_E = Probability of Preventing the Event
- $= P_{(I)\ INTERUPTION} \times P_{(N)\ NEUTRALIZATION}$
- C = Consequence Value

Note: If P_E is the probability of preventing the event then $[1-P_E]$ must be the probability of the adversary being successful

* The Design and Evaluation of Physical Security Systems, Garcia, Mary Lynn, Butterworth-Heinemann, 2001

14

Regarding risk, in general terms we know risk is a function of Vulnerability, Threat (sometimes called the Vuln – Threat pair), Likelihood or Probability, and Impact or Consequence

Risk is modeled as a function of Probability, Vulnerability, and Impact.

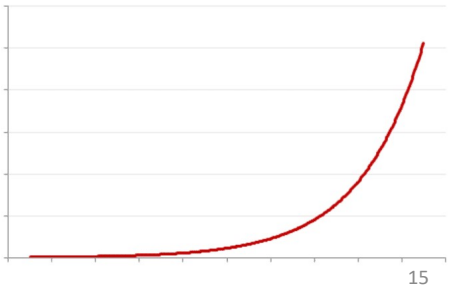
Let's see what that looks like on a risk matrix.

Source File:
Relating Risk & Vulnerability HANDOUT.pdf
Relating Risk and Vulnerability
Phillip Banks P. Eng. CPP
ASIS International 60th Seminar and Exhibits Atlanta, GA
September 29th to October 2nd, 2014

Risk matrix - (X, Y) cross product

- statistical calculation (e.g. $\frac{1}{2} x \frac{1}{2} = \frac{1}{4}$)
- renders an exponential pattern

		Impact				
		0.00	0.30	0.50	0.70	1.00
	Likelihood	V. Low	Low	Moderate	High	V. High
1.00	V. High	0.00	0.30	0.5	0.70	1.00
0.70	High	0.00	0.21	0.35	0.49	0.70
0.50	Moderate	0.00	0.15	0.25	0.35	0.50
0.30	Low	0.00	0.09	0.15	0.21	0.30
0.00	V. Low	0.00	0.00	0.00	0.00	0.00



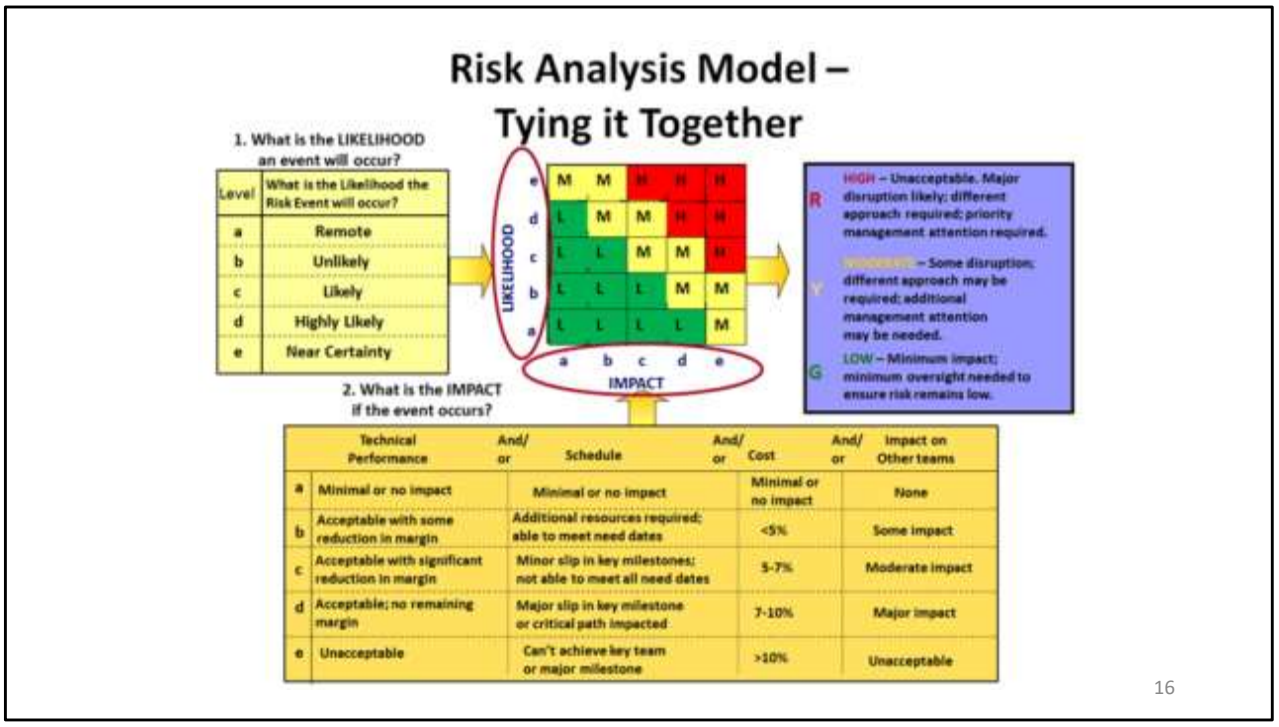
Likelihood and Impact values are multiplied together. What happens when you multiply linear values? Right, there's an exponential growth.

For example, when we multiply Moderate (0.5) times Moderate (0.5) we don't get 0.5 in the middle of the heat map; we get 0.25.

As a result, the color transitions exponentially. And, we get a non-symmetrical heat map. In fact, it appears more green than red. Only when we have an (X, Y) pair that is relatively high do we obtain a High. The effect is deceiving, unless it's necessary to model an exponential behavior.

We won't get into normal distributions, 1 sigma, 2 sigma, and 3 sigma standard deviations.

In the following slides we'll show academic and federal guidelines that support symmetrical risk maps.



Here's an acquisition risk example, where the red – green distribution is only slight skewed.

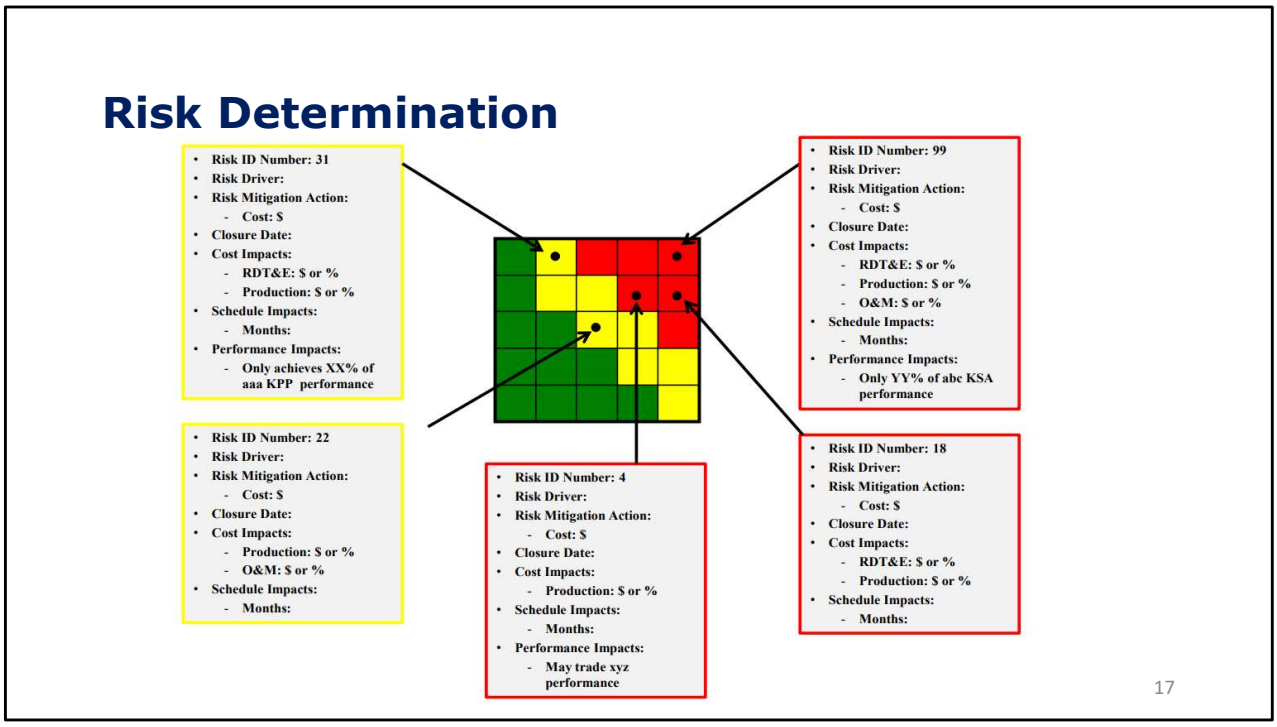
The message to leadership is: the majority of our systems are going to be characterized as low risk systems.

Source: Figure B-10. Risk Assessment Process
Risk Management Guide for DOD Acquisition

Fifth Edition (Version 2.0)

Defense Acquisition University

June 2003



Here's another Acquisition Risk matrix – also slightly skewed.

Ref: DoD Risk Management Guide for Defense Acquisition Programs, 7th Edition (Interim Release)

Risk Determination

Likelihood		Level of Impact				
		Very Low	Low	Moderate	High	Very High
		1	2	3	4	5
Very High	5					
High	4			I		
Moderate	3					
Low	2		C			
Very Low	1					A

Legend
Very High
High
Moderate
Low
Very Low

18

Here's an Excel spreadsheet image I discovered in a community knowledge repository called Knowledge Service.

File name: DoD RAR Final.xlsx
Identical to the image in the **DoD Risk Assessment Guide April 2014**

This too is non-symmetrical. The risk security posture is again more positive than what a normal distribution might render.

Source: DoD Risk Assessment Report (RAR) of Non-Compliant (NC) Security Controls.

Level of Risk Matrix

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	V. Low	Low	Mod	High	V. High
V. High	V. Low	Low	Mod	High	V. High
High	V. Low	Low	Mod	High	V. High
Mod	V. Low	Low	Mod	Mod	High
Low	V. Low	Low	Low	Low	Mod
V. Low	V. Low	V. Low	V. Low	Low	Low

Very Low: 7
Low: 8
Moderate: 5
High: 3
Very High: 2

PAGE I-1, NIST Special Publication 800-30, Revision 1

19

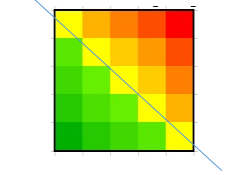
Here one from NIST SP 800-30, "Guide for Conducting Risk Assessments", September 2012

Would you say this is wrong? Or expected?

The 800-30 says, "The assessment scales in this appendix **can be used as a starting point** with appropriate tailoring to adjust for any organization-specific conditions."

Risk matrix - (X, Y) average

		Impact				
		0.00	0.30	0.50	0.70	1.00
	Likelihood	V. Low	Low	Moderate	High	V. High
1.00	V. High	0.50	0.65	0.75	0.85	1.00
0.70	High	0.35	0.50	0.60	0.70	0.85
0.50	Moderate	0.25	0.40	0.50	0.60	0.75
0.30	Low	0.15	0.30	0.40	0.50	0.65
0.00	V. Low	0.00	0.15	0.25	0.35	0.50



20

To avoid the exponential growth effect, let's try a linear calculation like then average of two values.

This is a trinary, or ternary, heat map, using Red, Yellow, and Green.

An (X, Y) average function makes the color transition vary linearly. As a result, the square graphic is symmetrical about the axis provided. There is an equal distribution of green versus the red distribution.

What do you think? Is this more honest?

Not statistical

The term *likelihood*, as discussed in this guideline, is not likelihood in the strict sense of the term; rather, it is a likelihood score. **Risk assessors do not define a likelihood function in the statistical sense.** Instead, risk assessors assign a score (or likelihood assessment) based on available evidence, experience, and expert judgment.

Combinations of factors such as targeting, intent, and capability thus can be used to produce a score representing the likelihood of threat initiation; combinations of factors such as capability and vulnerability severity can be used to produce a score representing the likelihood of adverse impacts; and **combinations of these scores can be used to produce an overall likelihood score.**

PAGE G-1, NIST Special Publication 800-30, Revision 1

21

Here's a note that touches on the idea that Risk assessments are NOT about statistical results.

In fact, the 800-30 states, that likelihood should be assigned a score (vice calculating one).

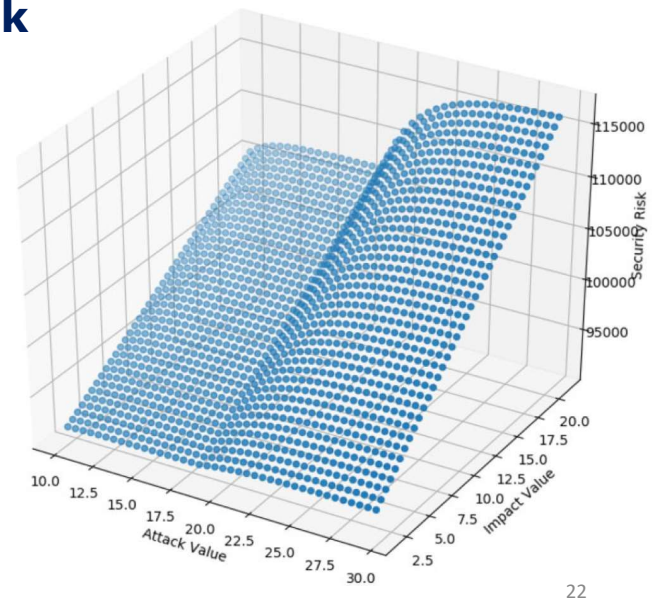
PAGE G-1, NIST Special Publication 800-30, Revision 1
"Guide for Conducting Risk Assessments", September 2012

Impact Value vs. Risk

X-axis: value of an attack to an adversary

Y-axis: impact of an attack to the defender

Z-axis: unmitigated Risk



22

I discovered this graph from a research paper in the Journal of Cybersecurity.

In this case, risk is a function of the impact value (Y-Z plane). And it's not exponential, but linear.

File name: **SMART risk evaluation tool.pdf**

Journal of Cybersecurity, 2020, 1–8
doi: 10.1093/cybsec/tyaa003
Research paper

SMART: security model adversarial risk-based tool for systems security design evaluation

Paul A. Wortman * and John A. Chandy

Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT, USA

*Correspondence address. E-mail: paul.wortman@uconn.edu

Received 1 January 2020; accepted 24 January 2020