The 4 Things to Radically Focus on to get your Security Program off the Ground

Curtis L. Blais - Cybera's Shared CISO
MAL, CCNA, CCNP, GCIA, GCFW, WCSP, CISSP, CRISC, CCSK
Harvard Cyber Risk Management
curtis.blais@cybera.ca

QR CODES

ENTP

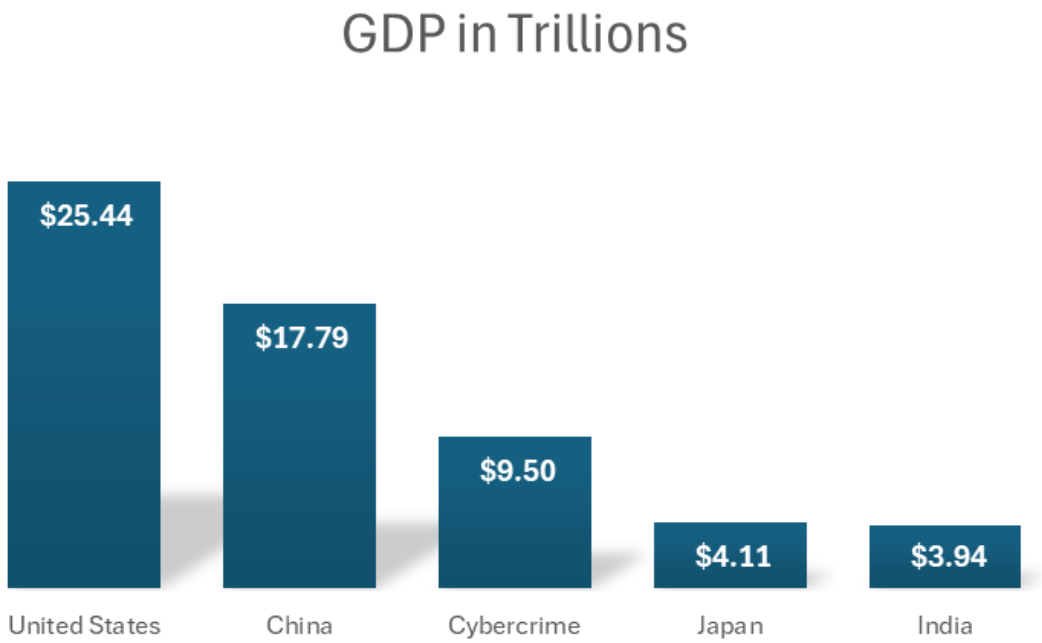
22,254

34,888

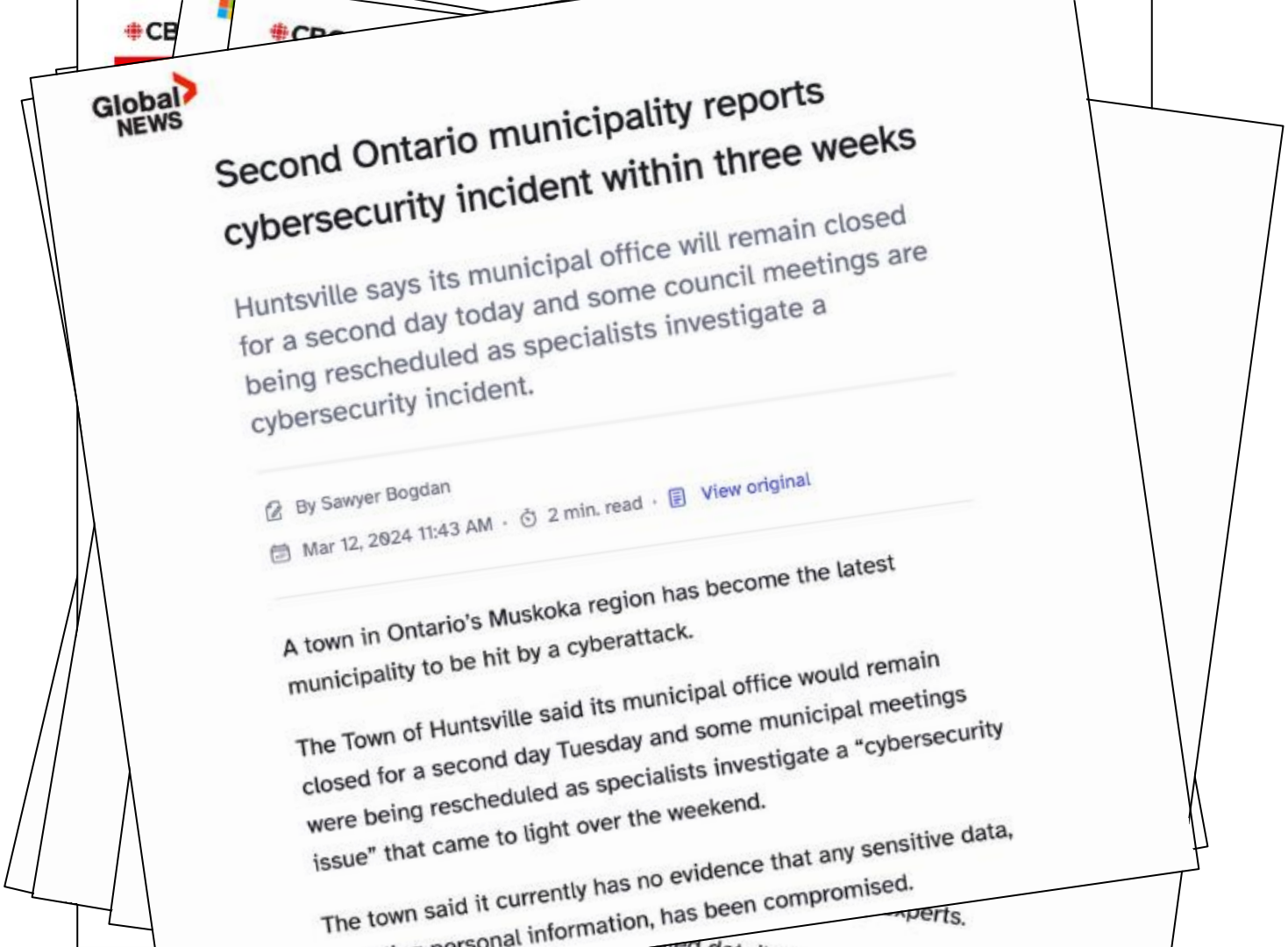
$9.5 Trillion

https://cybersecurityventures.com/cybersecurity-almanac-2024/

$9.5 Trillion



https://cybersecurityventures.com/cybersecurity-almanac-2024/



Global NEWS

Second Ontario municipality reports cybersecurity incident within three weeks

Huntsville says its municipal office will remain closed for a second day today and some council meetings are being rescheduled as specialists investigate a cybersecurity incident.

By Sawyer Bogdan

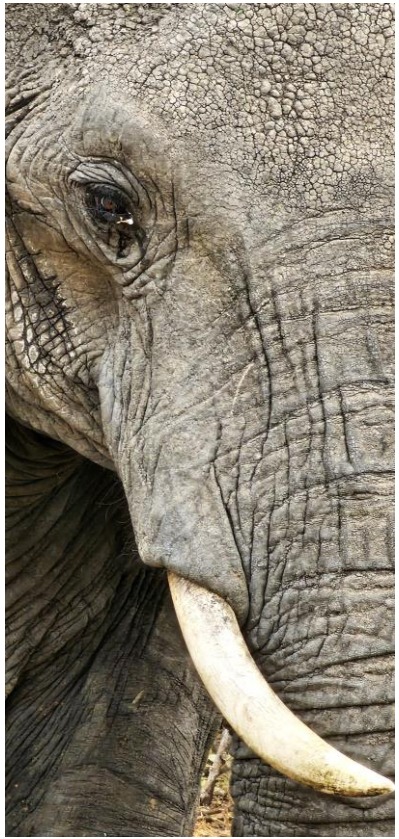
Mar 12, 2024 11:43 AM · 2 min. read · View original

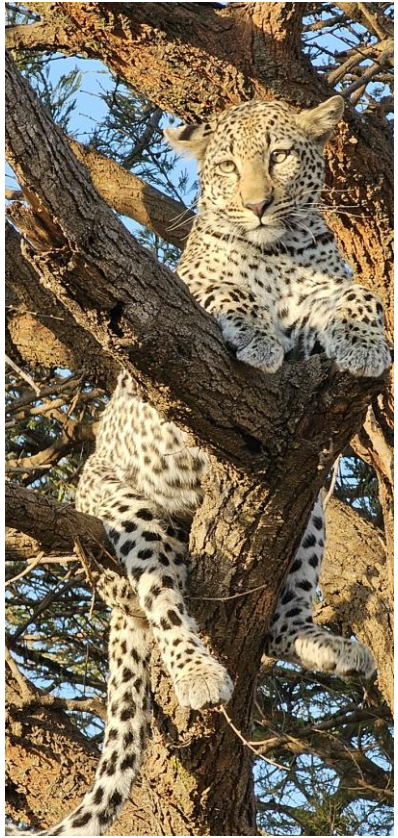
A town in Ontario's Muskoka region has become the latest municipality to be hit by a cyberattack.

The Town of Huntsville said its municipal office would remain closed for a second day Tuesday and some municipal meetings were being rescheduled as specialists investigate a "cybersecurity issue" that came to light over the weekend.

The town said it currently has no evidence that any sensitive data, personal information, has been compromised.

BLOG - Curt & Laureen - Africa 2023



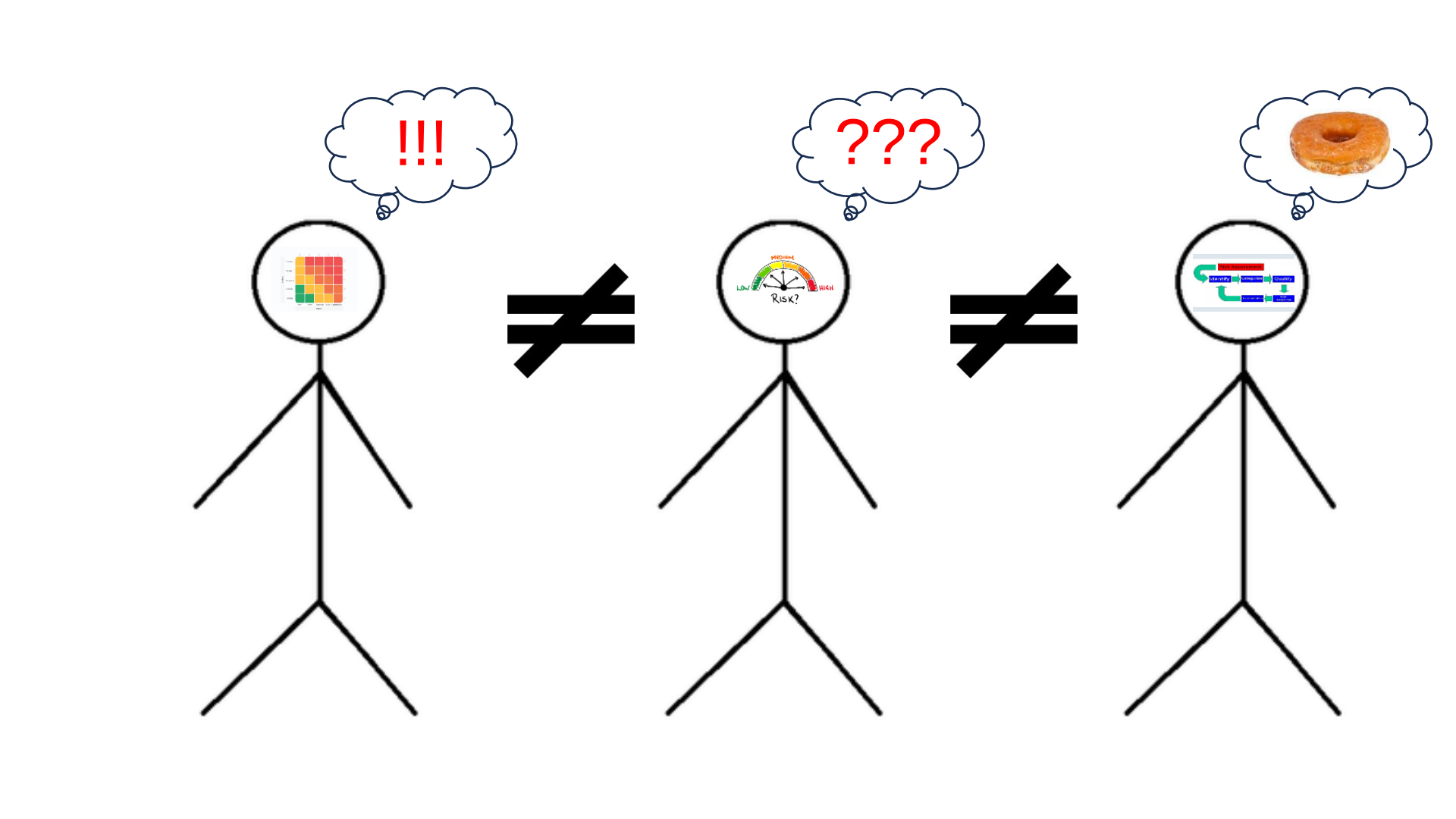



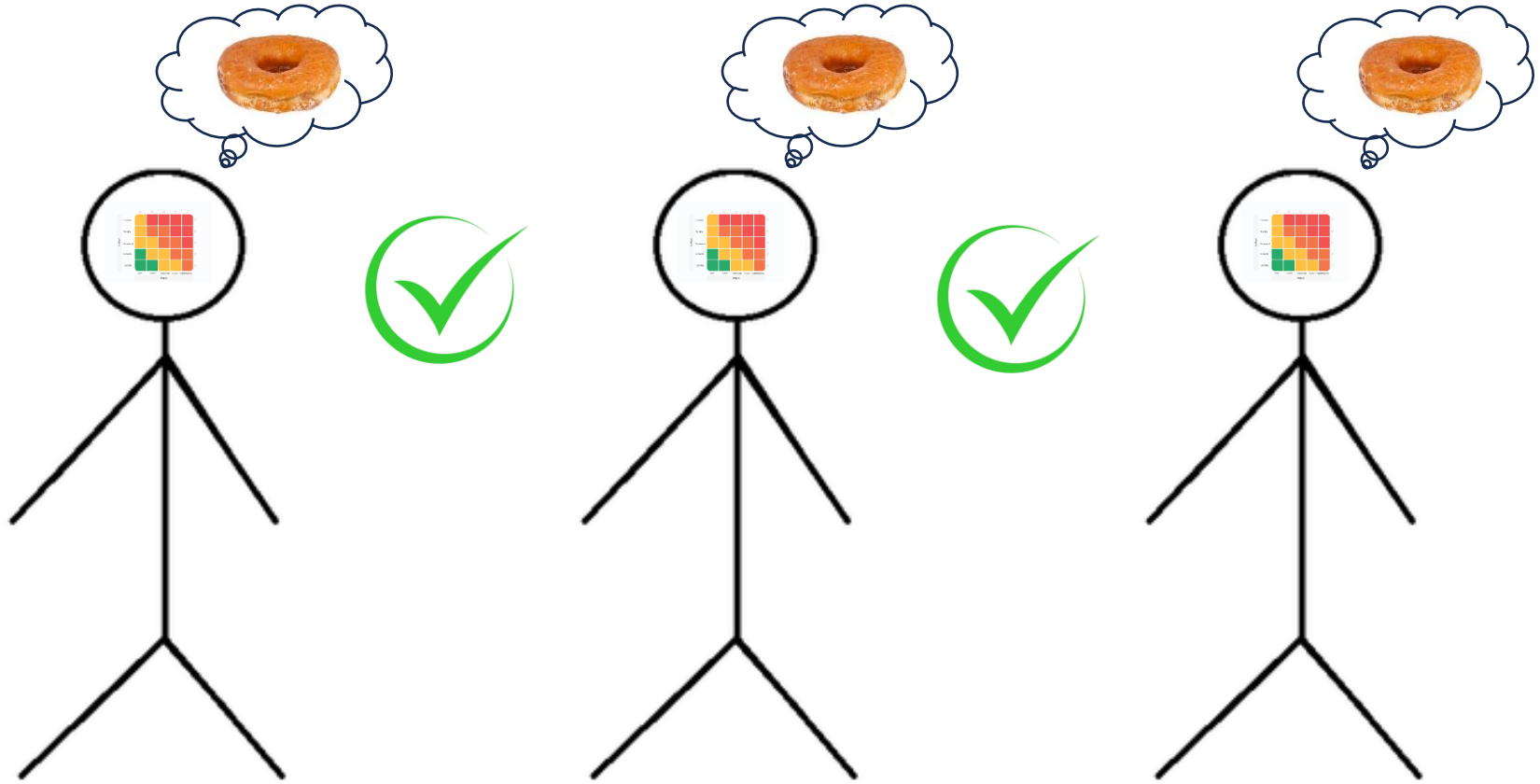
Lift | Weight | Drag | Thrust = FLIGHT

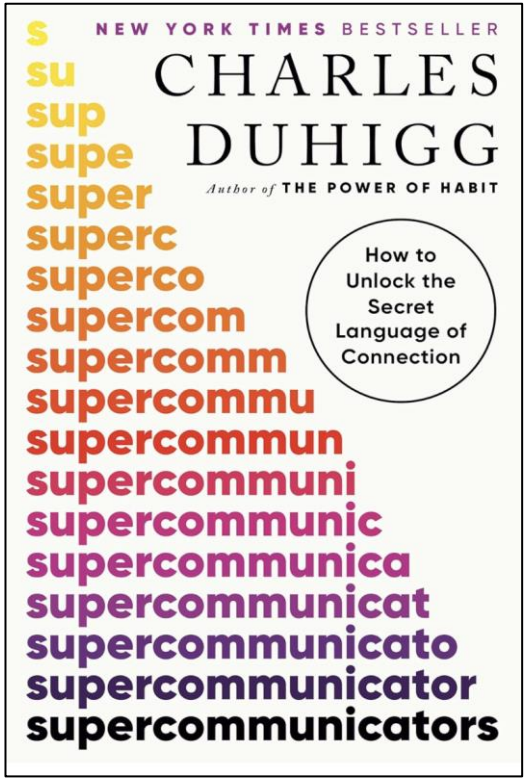
RISK
CLASS
DESIGN
CONTROL

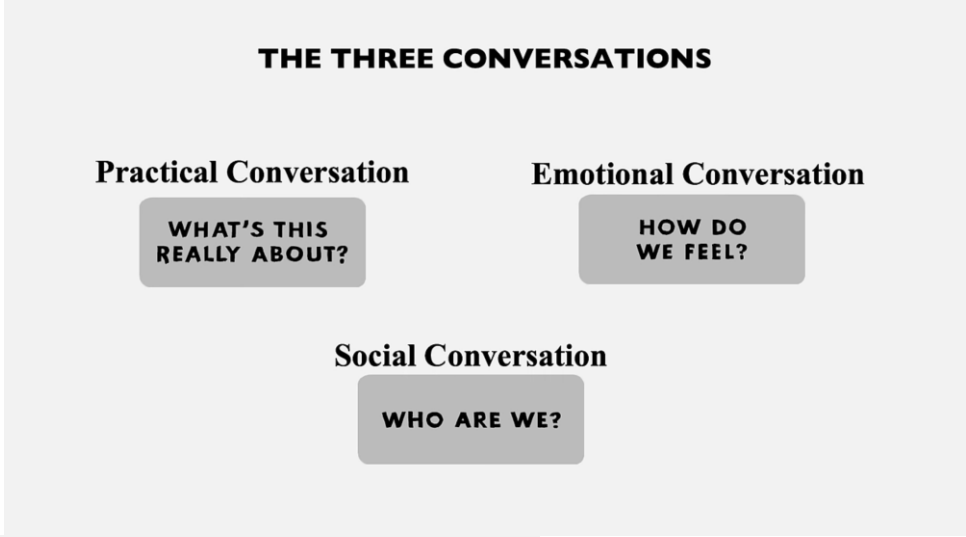
RISK

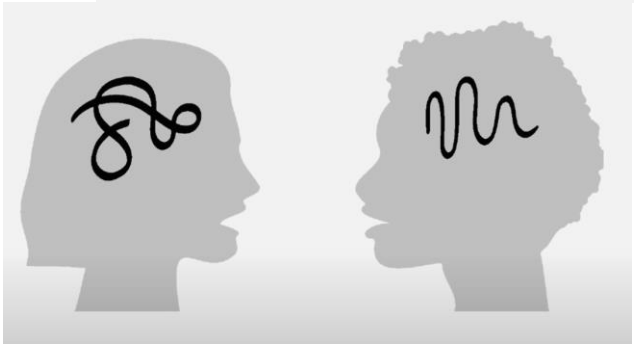

PM
AL
6:
RCA
AeroPress


!!!
???
MEDIUM
LOW
HIGH
RISK?









The science behind dramatically better conversations | Charles Duhigg | TEDxManchester
https://youtu.be/lg48Bi9DA54?si=vAX1zeajoaFvb2wd

LIKELIHOOD x IMPACT = RISK

LIKELIHOOD

Likelihood	Criteria
Very High 5	• Almost Certain • Up to once in two months or more • 90% or greater chance of occurrence over life of asset or project
High 4	• Likely • Once in 1 year up to once in 5 years • 65% up to 90% chance of occurrence over life of asset or project
Medium 3	• Possible • Once in 5 years up to once in 10 years • 35% up to 65% chance of occurrence over life of asset or project
Low 2	• Unlikely • Once in 10 years up to once in 25 years • 10% up to 35% chance of occurrence over life of asset or project
Remote 1	• Rare • Once in 25 years or more • < 10% chance of occurrence over life of asset or project

X

IMPACT

Impact	Category	Criteria
Extreme 5	FINANCIAL	Loss of over $4 million
	REPUTATIONAL	International long-term negative media coverage; game-changing loss of market share
	LEGAL or REGULATORY	Significant prosecution and fines, litigation including class actions, incarceration of leadership
	HEALTH	Significant injuries or fatalities to employees or third parties, such as customers or vendors
	PERSONNEL	Multiple senior leaders leave
	INFORMATION TECHNOLOGY	Significant loss or permanent damage to Information Systems; excessive downtime; over triple the expected RTO
High 4	FINANCIAL	Loss of $2 million up to $4 million
	REPUTATIONAL	National long-term negative media coverage; significant loss of market share
	LEGAL or REGULATORY	Report to regulator requiring major project for corrective action
	HEALTH	Limited in-patient care required for employees or third parties, such as customers or vendors
	PERSONNEL	Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
	INFORMATION TECHNOLOGY	Major loss or damage to Information Systems; major downtime; over double the expected RTO
Medium 3	FINANCIAL	Loss of $1 million up to $2 million
	REPUTATIONAL	National short-term negative media coverage
	LEGAL or REGULATORY	Report of breach to regulator with immediate correction to be implemented
	HEALTH	Out-patient medical treatment required for employees or third parties, such as customers or vendors
	PERSONNEL	Widespread staff morale problems and high turnover
	INFORMATION TECHNOLOGY	Some loss or damage to Information Systems; intermittent downtime; possible to achieve expected RTO
Low 2	FINANCIAL	Loss of $500,000 up to $1 million
	REPUTATIONAL	Local short term negative media coverage
	LEGAL or REGULATORY	Reportable incident to regulator, no follow up
	HEALTH	No or minor injuries to employees or third parties, such as customers or vendors
	PERSONNEL	General staff morale problems and increase in turnover
	INFORMATION TECHNOLOGY	Minimal loss or damage to Information Systems; minimal downtime; possible to exceed expected RTO
Minimal 1	FINANCIAL	Loss up to $500,000
	REPUTATIONAL	Local media attention quickly remedied
	LEGAL or REGULATORY	Not reportable to regulator
	HEALTH	No injuries to employees or third parties, such as customers or vendors
	PERSONNEL	Isolated staff dissatisfaction
	INFORMATION TECHNOLOGY	No significant loss or damage to Information Systems; very limited downtime; No need to enact RTO

=

RISK

Risk Metrics Heat Map		Consequence (Impact) Minimal 1	Low 2	Medium 3	High 4	Extreme 5
Likelihood: Very High (Almost Certain)	5	5	10	15	20	25
High (Likely)	4	4	8	12	16	20
Medium (Possible)	3	3	6	9	12	15
Low (Unlikely)	2	2	4	6	8	10
Remote (Rare)	1	1	2	3	4	5

Tolerance

Risk Score	Risk Rating
20 – 25	Catastrophic
12 – 16	Major
8 – 10	Moderate
4 – 6	Minor
1 – 3	Incidental

ACTION

	Risk Score	Risk Rating	Risk Definition	Activity Description
Risk Score and Treatment				
Above organization risk tolerance	20 – 25	Catastrophic	**Radically exceeds management's risk tolerance** Critical threat to the organization or its ability to achieve its mission or business objectives	**Eliminate, transfer or avoid immediately** Management must place a high priority on developing and implementing a strategy to reduce the level of residual risk
	12 – 16	Major	**Significantly exceeds management's risk tolerance** Serious threat to the organization or its ability to achieve its mission or business objectives	**Hedge and Monitor (7 - 30 days)** Management will place a priority on developing and/or implementing a strategy to reduce the level of residual risk
	8 – 10	Moderate	**Exceeds management's risk tolerance** Unlikely to pose a significant risk to the organization as a whole but could still impact on its ability to achieve its mission or business objectives	**Actively Manage (30-60 days)** Management will develop a strategy to reduce the level of residual risk over time to a level that falls within management's risk tolerance
RISK TOLERANCE THRESHOLD				
Meets organization risk tolerance	4 – 6	Minor	**Meets management's risk tolerance** Unlikely to have a significant impact on the organization as a whole or its ability to achieve corporate objectives	**Actively Monitor (semi-yearly or as required)** Management will, at a minimum, maintain existing risk management strategies to ensure residual risk remains within the risk tolerance
	1 – 3	Incidental	**Below management's risk tolerance** Unlikely to have any impact on the organization as a whole or its ability to achieve corporate objectives.	**Retain and Monitor Occasionally (yearly or as req.)** Management to maintain existing risk management strategies

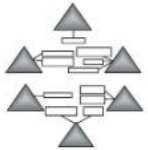
JL★ AIR FORCE JOURNAL of LOGISTICS

Volume XXII, Number 1

Lieutenant General Hallin Discusses Reengineering Air Force Logistics

Past Performance: Picking Winners

It makes good business sense to allow past performance evaluation in the selection of contractors. The begging question is then: How should it be implemented?



Depot Operations Modeling Environment

The DOME effort is aimed at addressing some of the most critical problems faced by Air Force logistics-related process redesign efforts.

Royal Flying Corps Logistic Organisation

The logistic organisation developed by the RFC and the support of deployed operations in France between 1914 and 1918.

Also in this issue:

- *Risk Matrix*
- *Operation JUST CAUSE*

Risk Matrix: An Approach for Identifying, Assessing, and Ranking Program Risks

Paul R. Garvey
Zachary F. Lansdowne

Introduction

Risk Matrix is a structured approach that identifies which risks are most critical to a program and provides a methodology to assess the potential impacts of a risk, or set of risks, across the life of a program. The approach was devised by the acquisition reengineering team at the Air Force Electronic Systems Center (ESC) in 1995. (4) Since January 1996, a number of ESC programs have implemented Risk Matrix.

To facilitate its use, The MITRE Corporation developed a Risk Matrix software application. New analytical features were also added as part of the software development. These include an automated way to cross-check the risk ratings produced by Risk Matrix, as well as an approach for measuring risk mitigation progress. Built in Excel 5.0, the application is cross-platform compatible and can be used on either the Macintosh or PC platforms. This article describes the original Risk Matrix, recently added analytical features, and the software application.

Original Risk Matrix

In Risk Matrix, a risk refers to the possibility that a program's requirement cannot be met by available technology or by suitable engineering procedures or processes. The approach focuses on the requirements-technology pair as the basis for identifying whether a risk exists to the program. A sample Risk Matrix is shown in Table 1. Once a risk (or set of risks) is identified, the subsequent steps in a Risk Matrix are: assess its potential program impacts, hypothesize the probability the risk will occur, rate the risk according to a predetermined scale, and document an action plan to manage/mitigate the risk.

A Risk Matrix is typically completed by a risk management Integrated Product Team (IPT) in a workshop environment. The participants are usually members of the program office and are familiar with the program's technical and programmatic issues, as well as with relevant technologies. They need to work together to identity the program risks and to make the impact and probability assessments. The results are then entered into the Risk Matrix software application, or simply recorded on paper in the appropriate columns. Table 1 illustrates the original Risk Matrix developed in 1995. (4) Each column is defined as follows:

- **Requirements**. List the program's requirements. Typically, these come from two main sources: high-level operational requirements, such as the Operational Requirements Document (ORD), and programmatic requirements, such as those listed in the Program Management Directive (PMD).
- **Technology**. List available technologies that would help meet each requirement. If the technology does not exist or is not mature enough to support the requirement, the probability of a risk occurring becomes higher.

	Requirement (Threshold)	Technology	Risk	I	P_r, %	R	Manage/Mitigate
1.	VHF Single Channel Communications	ARC-186	• Poor Design	C	0-10	M	• Demonstration as Part of Source Selection
2.	Talk SINCGARS	ARC-210 ARC-201 GRC-114	• Algorithm Misunderstood • ICD Problems	C	41-60	H	• Demonstration as Part of Source Selection
3.	Talk 100 Miles	ARC-210	• Antenna Performance	S	61-90	M	• Key Parameter of Test Program
4.	Go On A-10, F-16, JSTARS and ABCCC	Technology Currently Not Available	• Wrong Power Supply Ratings • Wrong Connectors • Cosite Problems	Mi	0-10	L	• Aircraft Surveys During Ground Team Meeting
5.	Control Radio With Control Head	N/A	• Hard to Get Pilot Consensus	Mi	91-100	H	• Control Head Demonstrations Early in Program
6.	Joint Program Office	N/A	• Different Users	S	41-60	M	• Information and Decision-Making System
7.	Schedule: 24 Months Delivery	N/A	• Integrated Circuit Lead Time	S	11-40	M	• Incentivize On-Time Delivery

Table 1. Sample Risk Matrix Chart

- **Risks**. Identify and describe the risks that might prevent available technology from meeting each requirement.
- **Impact (*I*)**. Assess the impact the risk could have on the program. A default scale is defined in Table 2.
- **Probability of Occurrence (P_o)**. Assess the probability the risk will occur. A default scale is defined in Table 3.
- **Risk Rating (*R*)**. Determine the risk rating (either Low, Medium, or High) by mapping each (I, P_o) pair into the default matrix shown in Table 4.
- **Manage/Mitigate**. The final step is to document the team's strategy to manage/mitigate the risk.

Borda Voting Method

Once a Risk Matrix is populated with a complete set of inputs, questions arise such as: Which risk is most critical? Where should resources be allocated to eliminate the most troublesome areas of the program? Because Table 4 supports only three distinct ratings (High, Medium, or Low), Risk Matrix's original rating method necessarily yields an ordering with many ties. In the case of the sample Risk Matrix chart in Table 1, two risks tie for first place (the High designations), four risks tie for the second place (the Medium designations), and one risk is in third place (the Low designation). In an actual application of Risk Matrix, seven risks tied for first place, thirty-two for second place, and nineteen for third place. With so many ties, it is difficult to isolate the most critical areas of risk from those that are less threatening to the program.

To deal with ties, we incorporated a simple technique from voting theory into the Risk Matrix software application. The technique is known as the Borda method. (2,5,6) When applied to Risk Matrix, the Borda method ranks risks from most to least critical on the basis of multiple evaluation criteria, as described next.

Let N be the total number of risks, which is the same as the number of rows in Risk Matrix. Let the index i denote a particular risk and the index k denote a criterion. The original Risk Matrix

Impact Category	Definition
Critical (C)	An event that, if it occurred, would cause program failure (inability to achieve minimum acceptable requirements).
Serious (S)	An event that, if it occurred, would cause major cost/schedule increases. Secondary requirements may not be achieved.
Moderate (Mo)	An event that, if it occurred, would cause moderate cost/schedule increases, but important requirements would still be met.
Minor (Mi)	An event that, if it occurred, would cause only a small cost/schedule increase. Requirements would still be achieved.
Negligible (N)	An event that, if it occurred, would have no effect on the program.

Table 2. Risk Matrix Impact Assessments (Illustrative Definitions)

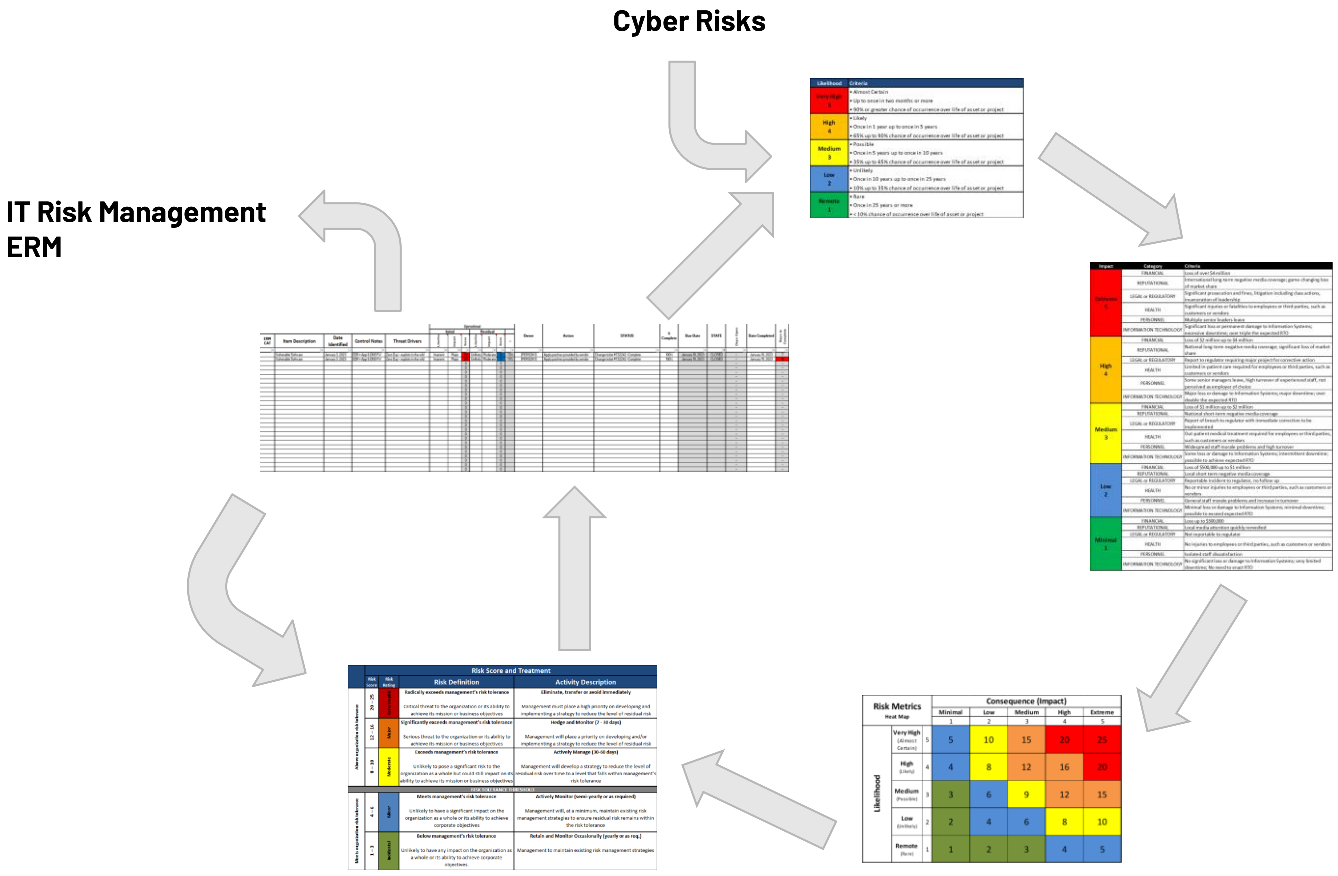
Probability Range	Interpretation
0-10%	Very Unlikely to Occur
11-40%	Unlikely to Occur
41-60%	May Occur About Half of the Time
61-90%	Likely to Occur
91-100%	Very Likely to Occur

Table 3. Probability of Occurrence (P_o)c Illustrative Interpretations

	Negligible	Minor	Moderate	Serious	Critical
0-10%	Low	Low	Low	Medium	Medium
11-40%	Low	Low	Medium	Medium	High
41-60%	Low	Medium	Medium	Medium	High
61-90%	Medium	Medium	Medium	Medium	High
91-100%	Medium	High	High	High	High

Table 4. Possible Risk Rating Scale (*R*)

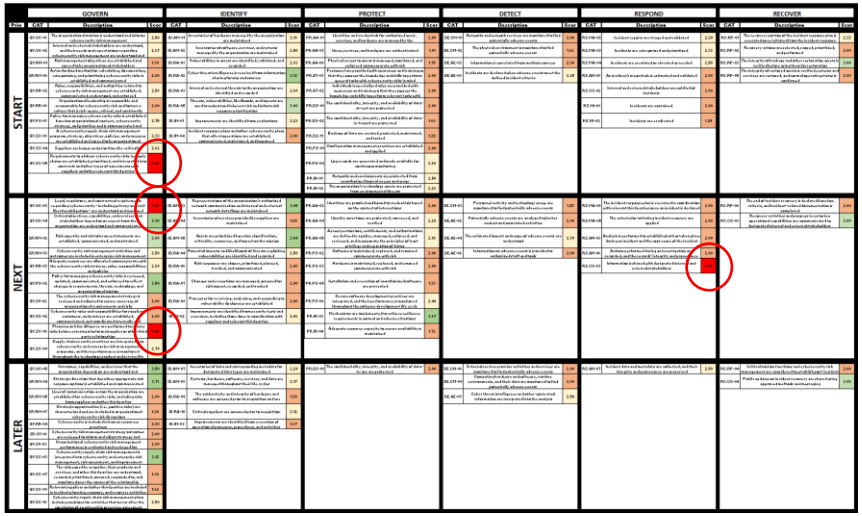
					Operational															
					Initial			Residual												
ERM CAT	Item Description	Date Identified	Control Notes	Threat Drivers	Likelihood	Impact	Score	Likelihood	Impact	Score	%	Owner	Action	STATUS	% Complete	Due Date	STATE	Days Open	Date Completed	Days to Complete
	Vulnerable Software	January 3, 2023	EDR + App & DNS FW	Zero Day - exploits in the wild	Imanent	Moderate	15	Unlikely	Moderate	6	-60%	[PERSON 1]	Apply patches provided by vendor	Change ticket #732242 -Complete	100%	February 2, 2023	CLOSED	-	January 10, 2023	7
	Vulnerable Software	January 3, 2023	EDR + App & DNS FW	Zero Day - exploits in the wild	Imanent	Extreme	25	Possible	Moderate	9	-64%	[PERSON 1]	Apply patches provided by vendor	Change ticket #732242 -Complete	100%	January 10, 2023	CLOSED	-	January 15, 2023	12
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-
							0			0								-		-

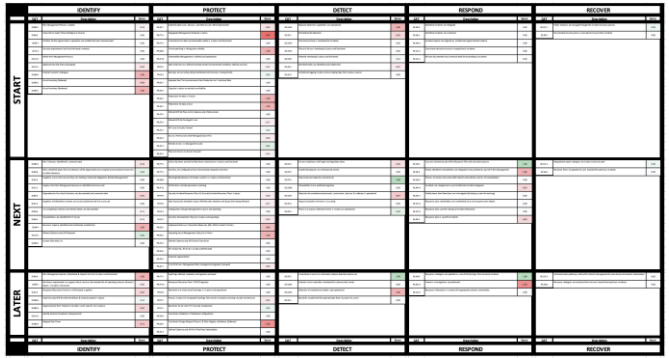

Cyber Risks
IT Risk Management
ERM
Risk Metrics
Heat Map
Consequence (Impact)
Minimal 1
Low 2
Medium 3
High 4
Extreme 5
Likelihood
Very High (Almost Certain) 5: 5 10 15 20 25
High (Likely) 4: 4 8 12 16 20
Medium (Possible) 3: 3 6 9 12 15
Low (Unlikely) 2: 2 4 6 8 10
Remote (Rare) 1: 1 2 3 4 5
Risk Score and Treatment
Risk Definition
Activity Description
Radically exceeds management's risk tolerance
Eliminate, transfer or avoid immediately
Significantly exceeds management's risk tolerance
Hedge and Monitor (7 - 30 days)
Exceeds management's risk tolerance
Actively Manage (30-60 days)
Meets management's risk tolerance
Actively Monitor (semi-yearly or as required)
Below management's risk tolerance
Retain and Monitor Occasionally (yearly or as req.)

250 Question
NIST CSF 2.0
Web Based Assessment

1 or below	Red
2 or below	Orange
3 or below	Yellow
3	Light Green
4 or below	Medium Green
5 or below	Dark Green

CMMI





RECOMMENDATIONS

1.
2.
3.
4.

RISK

"The Board doesn't speak too many languages,
but two they speak very well are: Business & Risk."
~ Gerrit Bos

- Work from a common RISK understanding
- Likelihood x Impact = Risk → Action (KIS)
- Risk Register

CLASS


https://stockcake.com/i/excited-classroom-chaos_1220136_1050201


https://stockcake.com/i/overwhelmed-by-paperwork_265460_52545

Performance
Classification
Improve
Text
Model
Task
Use
Data
More
Specific
Ensemble
Accuracy
Granular
Different
Topic
Multiple
Machine
System
Trained
Domain
Approach
Learning
Each
Adaptation
Article
Interpretability
Identify
Emotion
Handling
Overall
Important
Classifies
Pipeline
Understanding
Result
Efficient
Benefits
Accurate
Help
Entity
Lead
General
Outliers
Detect
Words
Combining
Given
Labels
Deploying
Better
Noisy
Time
Becomes
Overfitting
Miss
Discusses Case
Advantage
Natural
Multi
Patterns
Plot
Individual
Parallel
Describe
Features
Mentioned
Negative
Robust
Highlights
Reduced
Enable
Trees
Metrics
Practitioners
Leveraging
Weaknesses
Strengths
Many
Particular
Certain
Focuses
Risk
Faster
Way
Relevant
Tailor
Errors
Gain
Rapid
Areas
Visual
Picture
Behind
Suitable
Support
Biases
Deep
Outputs
Good
Characters
Prediction
Related
Focus
Descriptive
Occurs
Assign
Enhanced
Real
Less
Wide
Content
Highly
Unseen
Drift
Large
Recognition
Critical
Aspect
World
Goal
Capture
Range
Language
Structure
Maintain
Extract
Soundtrack
Requirements
Positive
Common
Insights
Additional
Determine
Provide
Based
Main
Underlying
Stable
Techniques
Complete
Analysis
Tackle
Contains
Reviews
Presence
Saving
Sensitive
Challenges
Fewer
Offer
Incremental
Customizable
Achieved
Adept
Average
Solution
Strategies
Quickly
Manage
Confidence
Context
Suited
Examining
Resilient
Named
Variances
Potential
Scalable
Vector
Capable
Jargon
Particularly
Domain
Accurate
Entity
Trained

From an information security context, classification is:

“The grouping of organizational data into categories of similar sensitivity”

STANDARD	DATA CLASSIFICATION
Owner: **Information Technology**	Approved Date: **DRAFT**

INFORMATION CLASSIFICATION MATRIX (in order from the least to the most restrictive)

Classification	Definition	Examples (Not limited only to the example provided)	Risk Impacts
Public	• Non-proprietary information that is created in the normal course of business that is unlikely to cause harm. • Available to the general public	• Corporate public website • Communication materials such as brochures, advertising, sponsorships, Annual report (printed version) • Approved Policy Documents • Student name, Major/Degree/Program • Campus map showing buildings, names, addresses, parking, lighted pathways, emergency phones, etc. • Employee's workplace name, business contact information	• Little or no impact • Minimal inconvenience if not available.
Protected [Protected A] (Default Class)	• Protected information may include business information about how we effectively operate and conduct business as well as non-personal information. • Access limited to individuals (employees and contractors, sub-contractors and agents) possessing a need to know for business-related purposes (role-based access). • Information is appropriately secured and not accessible by the public.	• Draft Policy and planning documents • Business procedure manuals • Staff meetings agendas/minutes • Internal communications • Application configuration and reference data (incl. flags, logically deleted and date stamps related to the system attributes • As of dates (incl. effective date, termination date) • Individual grades, academic transcript, class schedule, student coursework and examinations • Student ID # / Employee ID #	• Unfair competitive advantage • Low levels of financial loss to the enterprise • Disruption to business if not available.
Confidential [Protected B]	• Personal information that includes data not publicly available, financial information or sensitive information uniquely assigned to an individual (in many cases for their lifetime and of high importance, even external to CURTIS U), personal health related information. • Details concerning the effective operation of CURTIS U. • Business or financial/business information provided to CURTIS U in confidence. • Access and/or ability to input or change the information is limited to individuals in a specific function, group or role, for business-related purposes.	• Personal enrolment information (full name, birth date, death date, gender, height/weight, etc.) • Demographic information (individual's street address and postal code, city, province, e-mail address, individual's contact phone number(s), signature, photograph, citizenship/ immigration status) • Previous employer • Personal bank acct info - Electronic Funds Transfer (EFT), including transit number • Employee Salary / Home Address • Passwords • Personal Health Number (PHN) of individual • Social Insurance Number (SIN) • Medical history information (diagnostic and treatment) • Personnel files – HR related information • Third party business information submitted in confidence (in quotations or bids, billing rates of individuals) • Bills for an individual or organization • Internal documentation: marketing & unpublished academic research, survey results, faculty plans, patent applications • Payment Card Information • Driver's license/passport information • Institutional Financial records / Donor records • FOIP files • Solicitor-client privileged material • Network/Digital Security configurations/architectures or logging information	• Loss of reputation or competitive advantage and partnerships • Loss of confidence in CURTIS U products or services • Loss of personal or individual privacy, humiliation and reputational harm • Loss of trade secrets or intellectual property • Loss of business opportunity • Damage to partnerships • Possible legal action or media attention • Risk of identity theft/ financial loss • Loss of employment
Restricted [Protected C]	• Information whose loss, corruption or unauthorized disclosure would severely harm the company's reputation or business position resulting in financial, reputation or legal loss. • Access is specific to a named individual and is very limited. • The explicit approval of the information owner is required to release this information, even to those with a need to know.	• Executive documents • Agreements/Signed Contracts • Government briefing documents • Annual report prior to public release • Strategic Plan • Criminal investigations or litigation • Shared secrets & Cryptographic private keys	• Significant damage, including corporate reputation loss • Significant financial loss to CURTIS U • Compromise of government contracts/negotiations • Destruction of relationships with major customers • Compromise of legal position • Loss of life • Serious injury • Loss of public safety

Why is this important?

1. Used throughout the CONTROL Section
2. Provides the framework to have productive discussions
3. Demonstrates a consistent approach to security treatment in an audit situation

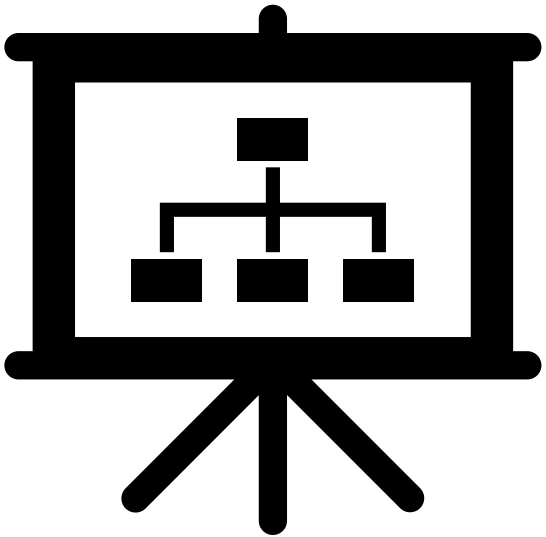
CLASS

“In all chaos there is a cosmos, in all disorder a secret order.”

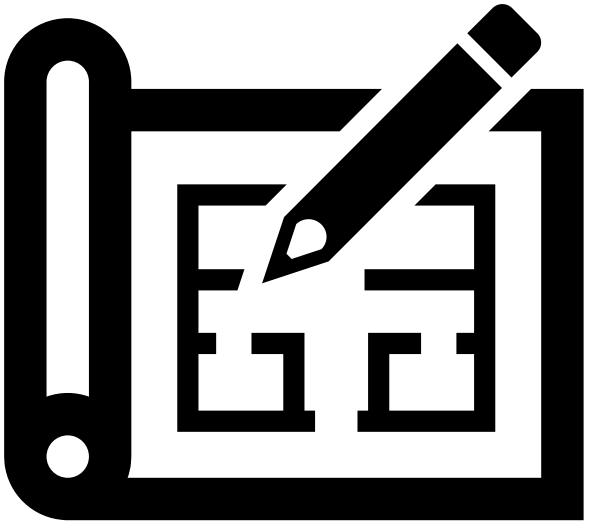
~Carl Jung

- Not Records Management
- Tagging EVERYTING is not required
- Critical for CONTROLS

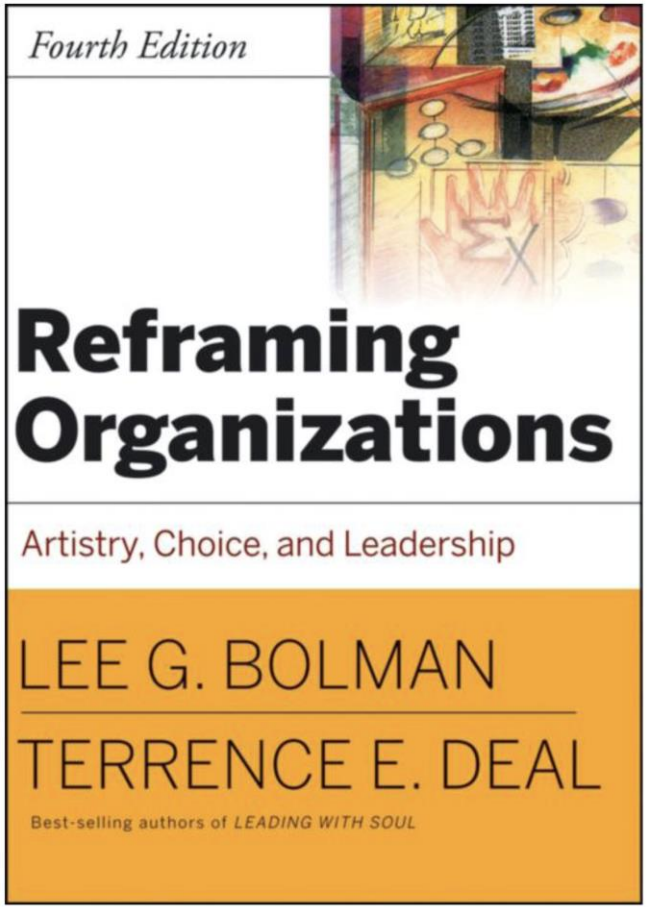
DESIGN



ORGANIZATION

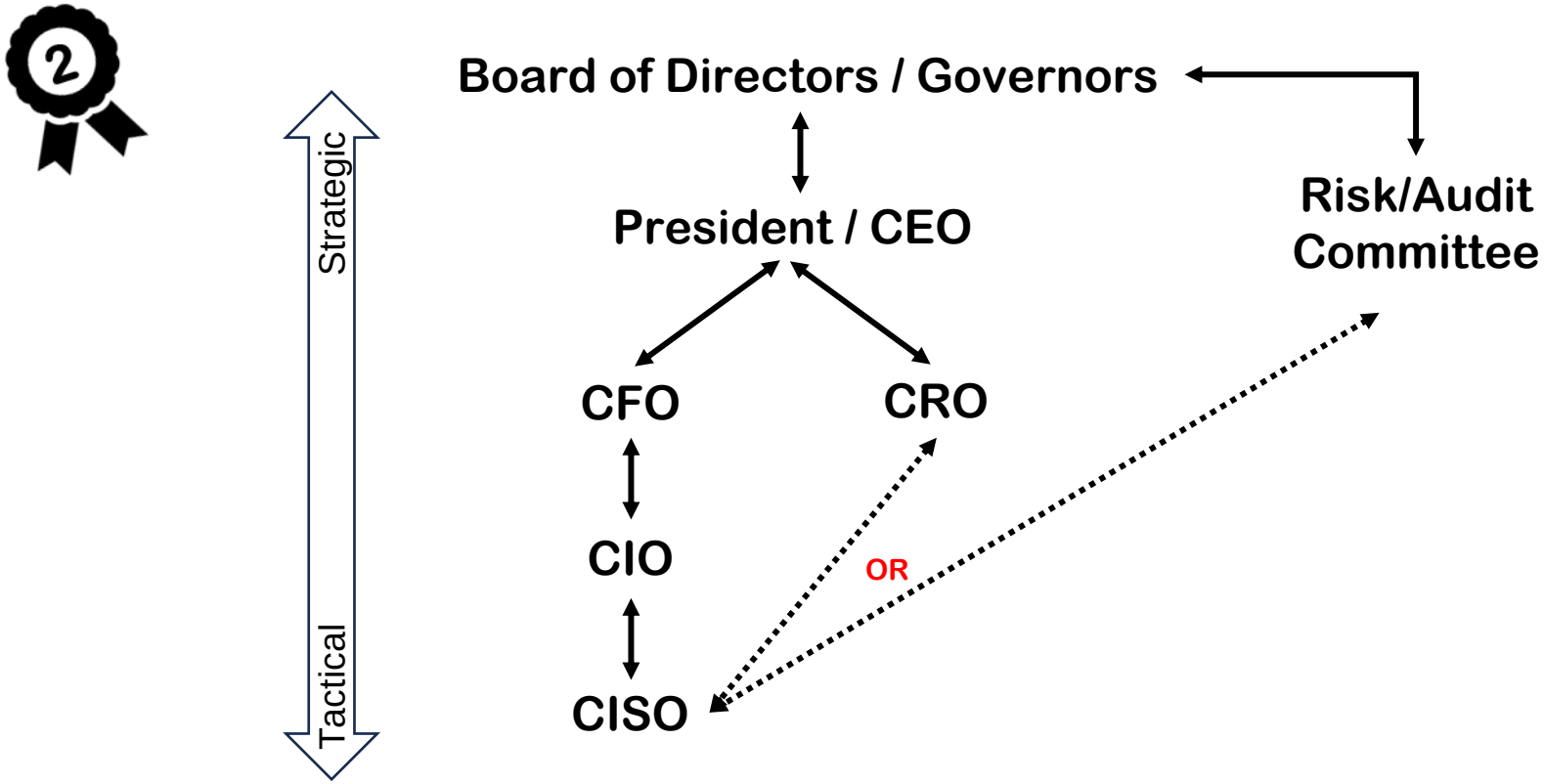


ARCHITECTURE

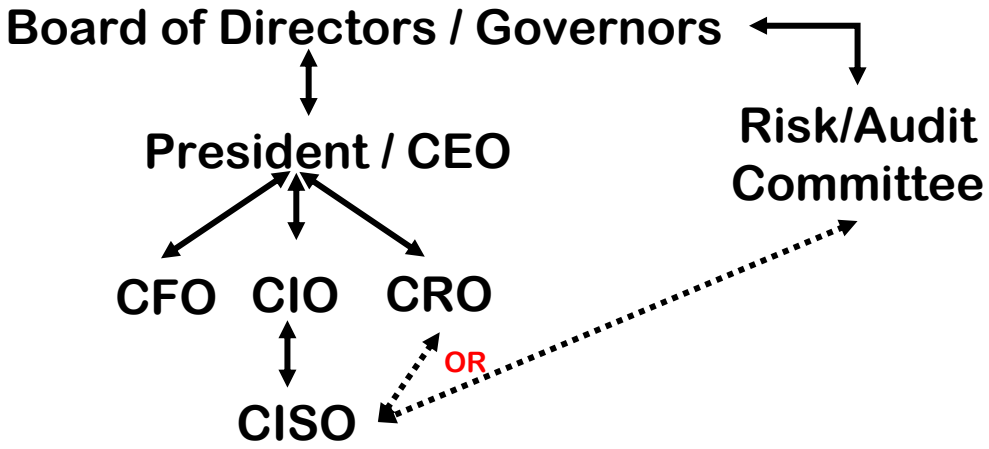


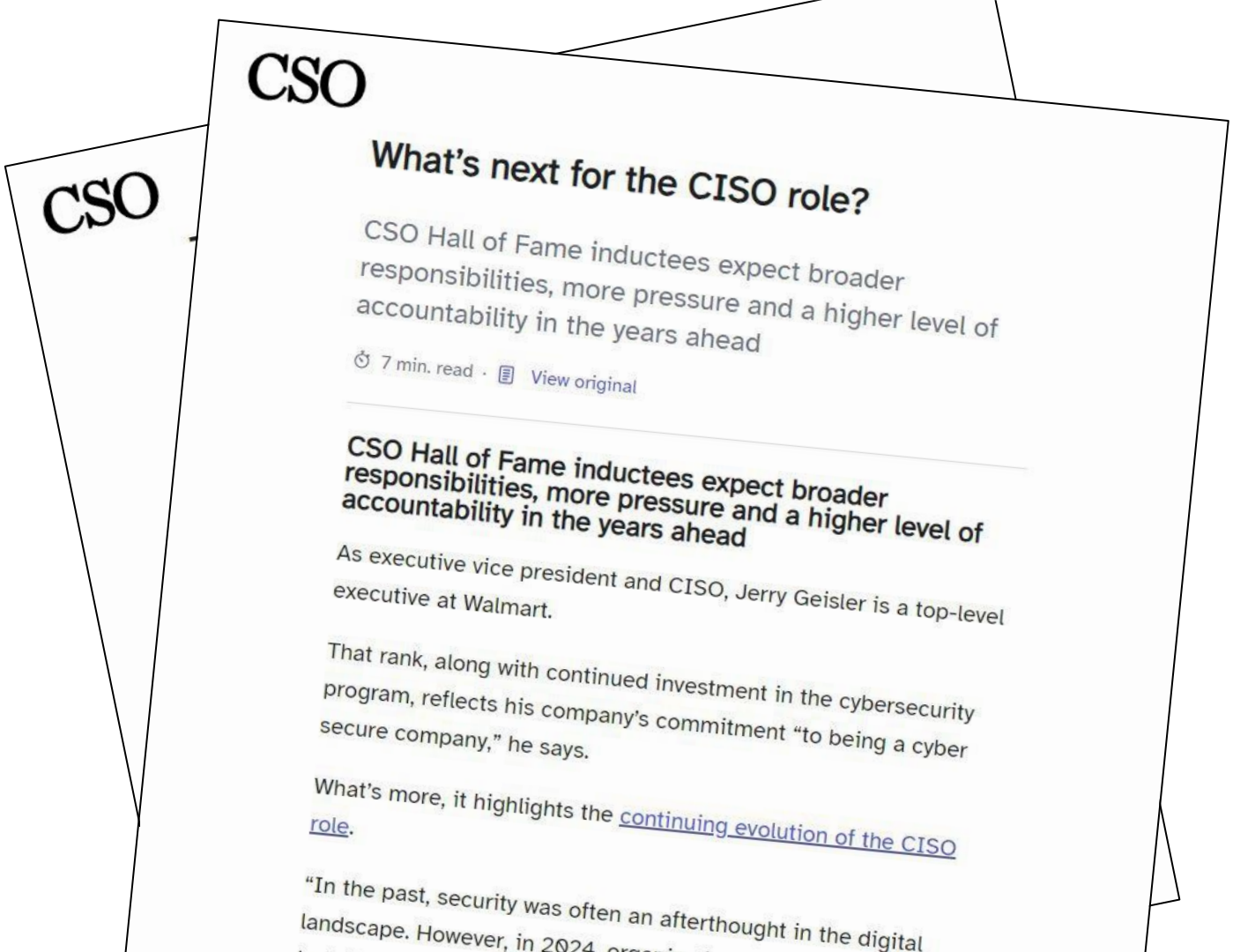
How does structure influence what happens in the workplace?

Essentially, it is a blueprint for officially sanctioned expectations and exchanges among internal players (executives, managers, employees) and external constituencies (such as customers and clients).


2
Strategic
Tactical
Board of Directors / Governors
President / CEO
Risk/Audit
Committee
CFO
CRO
CIO
OR
CISO


Strategic
Tactical


Board of Directors / Governors
President / CEO
Risk/Audit Committee
CFO
CIO
CRO
OR
CISO


CSO

What's next for the CISO role?

CSO Hall of Fame inductees expect broader responsibilities, more pressure and a higher level of accountability in the years ahead

7 min. read · View original

CSO Hall of Fame inductees expect broader responsibilities, more pressure and a higher level of accountability in the years ahead

As executive vice president and CISO, Jerry Geisler is a top-level executive at Walmart.

That rank, along with continued investment in the cybersecurity program, reflects his company's commitment "to being a cyber secure company," he says.

What's more, it highlights the continuing evolution of the CISO role.

"In the past, security was often an afterthought in the digital landscape. However, in 2024, organ

Strategic

Tactical

Board of Directors / Governors

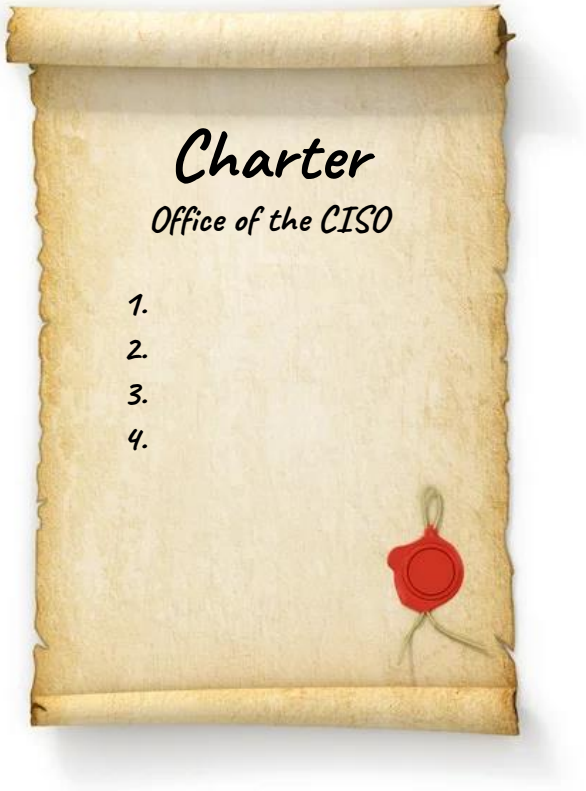
President / CEO

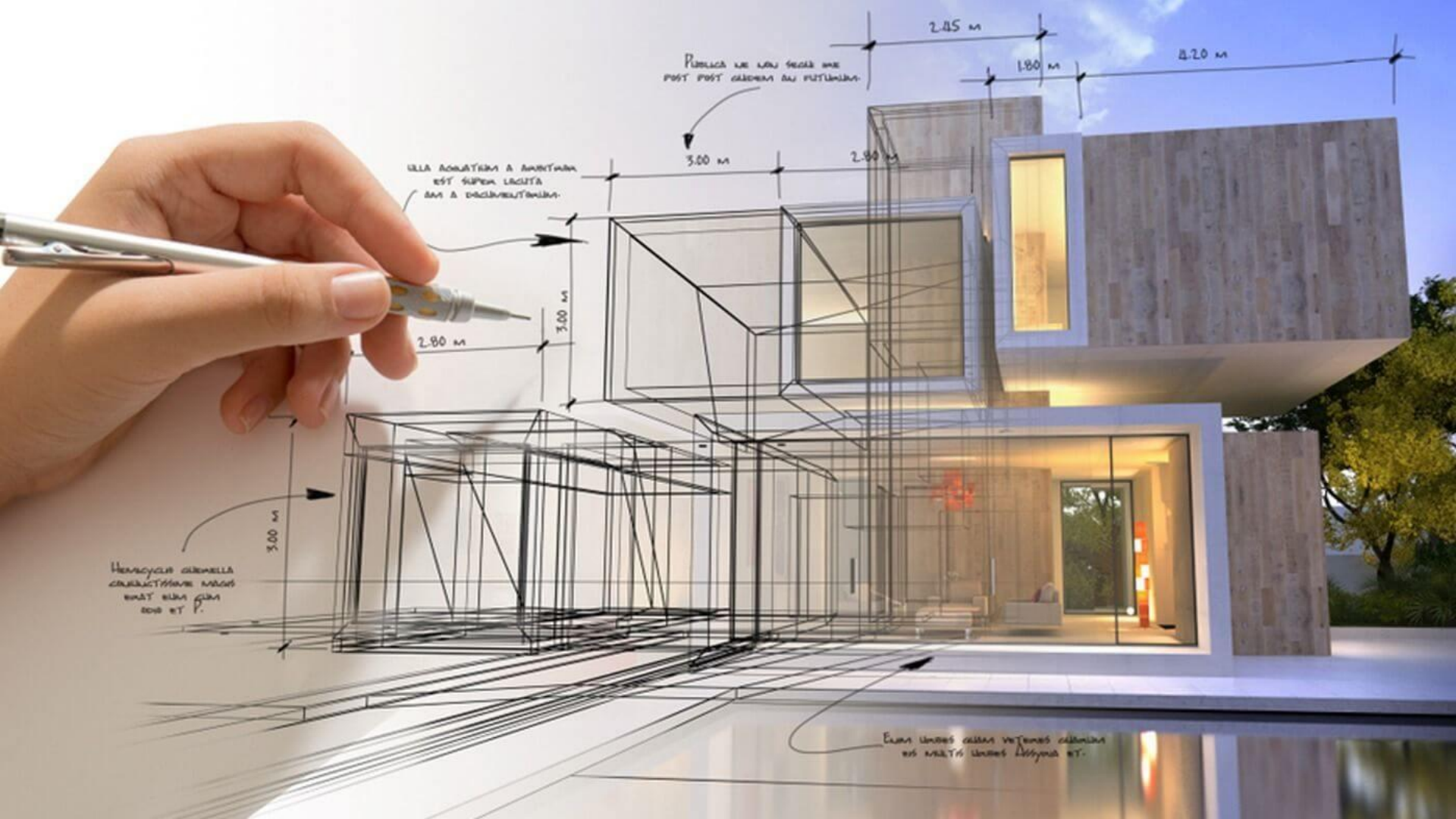
CFO **CISO** **CRO**

Risk/Audit Committee

Set up a Charter for the CISO

1. Provides mandate
2. Establishes authority
3. Makes way for compliance



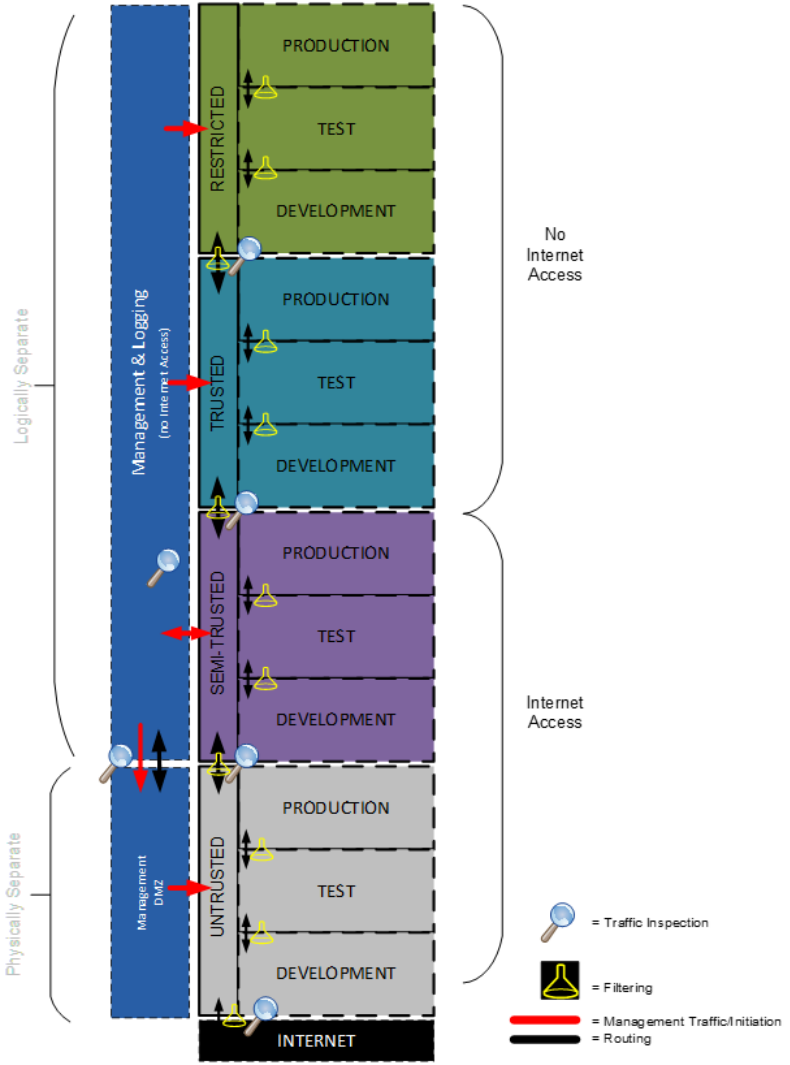

2.85 m
1.80 m
8.20 m
3.00 m
2.80 m
3.00 m
2.80 m
3.00 m

CISO establishes an: **Operational Model for Security Architecture**

- Contributes to Enterprise Architecture
- Veto capability

5 Sections:

- Untrusted
- Semi-Trusted
- Trusted
- Restricted
- Management x 2



DESIGN

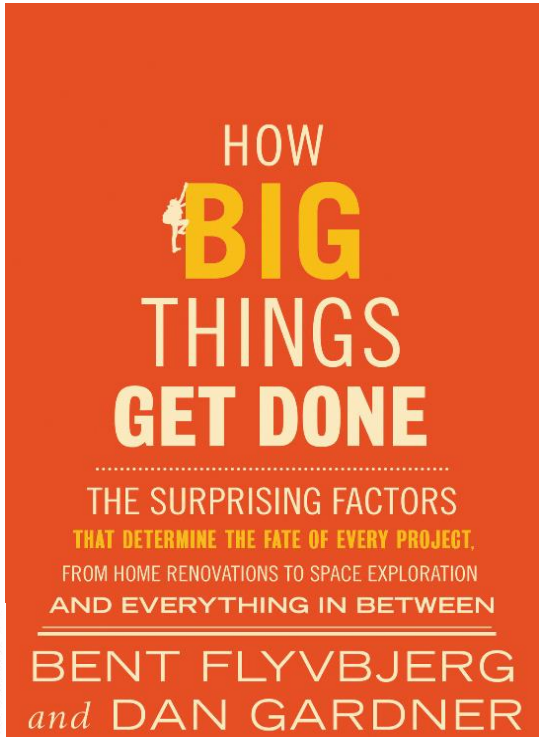
The details are not the details. They make the design.
~Charles Eames

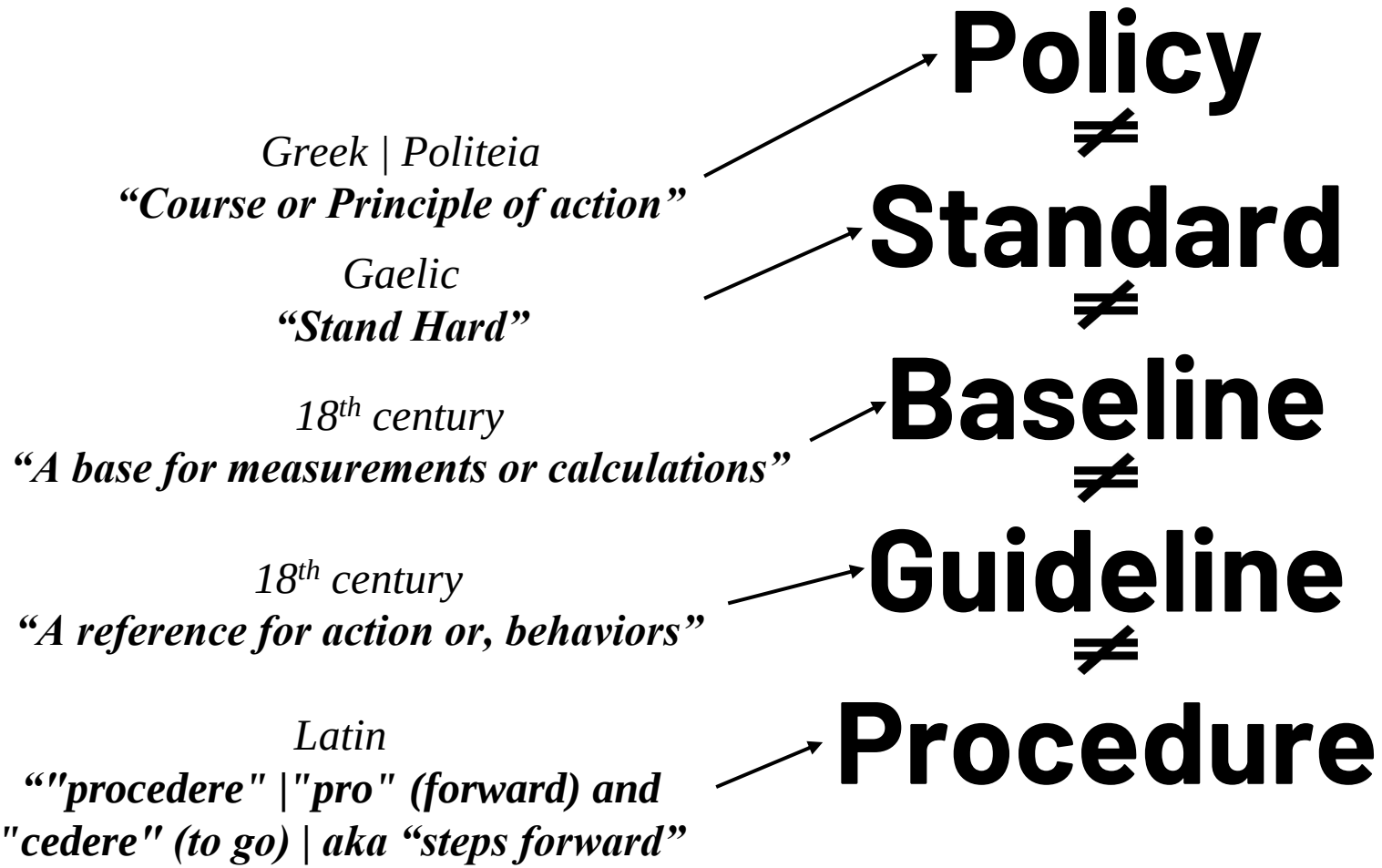
- Organizational structures are important
- CISO set/validate compliance with Standards (Charter)
- Operational Model for Security (What)
- Data is at the most protected level

CONTROL

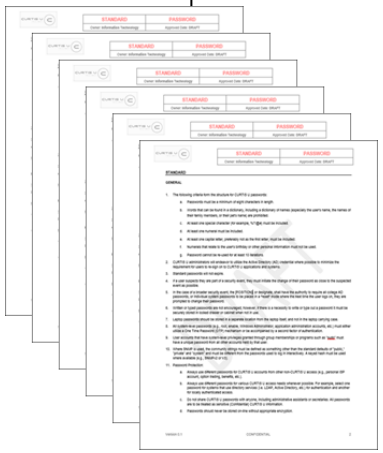

Organizational Strategy & Business Objectives
Line of Business Strategy & Business Objectives
IT Governance Framework
[COBIT]
Policy
Policy
IT Strategy
App Dev
InfoSec
PMO
Change Mgmt.
Vendor Mgmt.
QA
OPS
IT Arch.
IT GRC
HR
STRATEGY
STANDARDS
GUIDELINES
PROCESSES
CMMI
ISO-9001
OWASP
ISO-900X
ISO-27001
PCI / NIST
ITIL
PMBOK,
Prince, etc.
NIH, IEEE,
TOGAF
Zachman
ITIL
COBIT,
ISO-31000,
PIPA, etc.
VM Best
Practice
HR Best
Practice

“Modularity is a clunky word for the elegant idea of big things made from small things.”

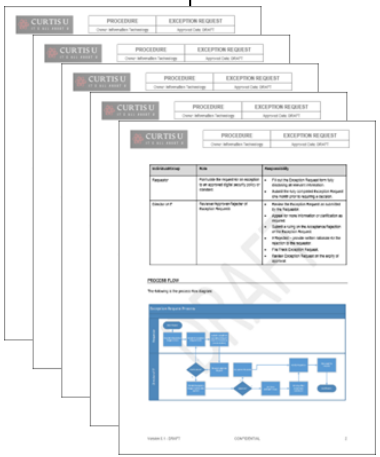



Policy
≠
Standard
≠
Baseline
≠
Guideline
≠
Procedure
Greek | Politeia
"Course or Principle of action"
Gaelic
"Stand Hard"
18th century
"A base for measurements or calculations"
18th century
"A reference for action or, behaviors"
Latin
"'procedere" |"pro" (forward) and "cedere" (to go) | aka "steps forward"

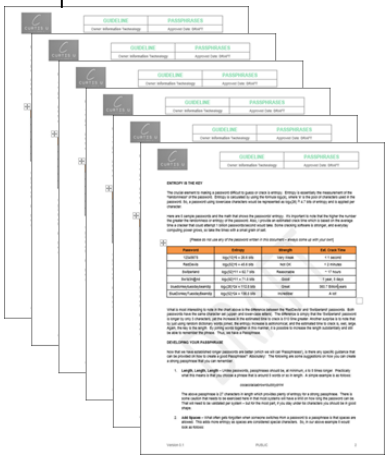
Policy



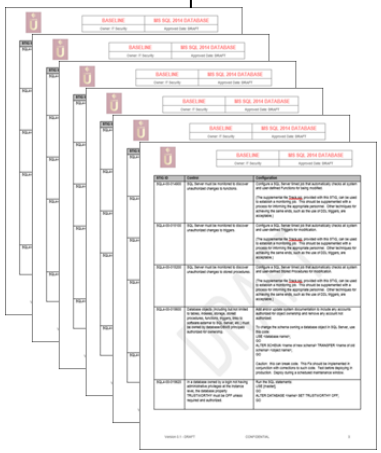
Standards



Procedures



Guidance



Baselines

STANDARDS
STANDARD - Acceptable Use
STANDARD - Account Lockout
STANDARD - Backup
STANDARD - Cloud Vendor Security
STANDARD - Cryptographic Key Management
STANDARD - Data Classification
STANDARD - Data Encryption
STANDARD - Data Residency
STANDARD - Data Retention
STANDARD - Data Transmission
STANDARD - Database Security
STANDARD - Electronic Media Disposal
STANDARD - Guest Wireless
STANDARD - IT Change Management
STANDARD - Logging/Monitoring
STANDARD - Major Risk Travel
STANDARD - Malicious Software Prevention Detection Eradication
STANDARD - Mobile Device Management
STANDARD - Network Security
STANDARD - Passwords
STANDARD - Patch & Vulnerability Management
STANDARD - Physical IT Security
STANDARD - Privileged Account Creation & Management
STANDARD - Remote Access
STANDARD - Risk Management
STANDARD - Security Incident Response
STANDARD - Security Training & Awareness
STANDARD - User Account Creation & Management
STANDARD - Wireless LAN
STANDARD - Zones Architecture

PROCEDURES
PROCEDURE - Exception Request
PROCEDURE - Third Party Disclosure Approval
PROCEDURE - Security Incident Response
PROCEDURE - Risk Management
PROCEDURE - IT Change Management

BASELINES
BASELINE - Android 5
BASELINE - Android 6
BASELINE - App Server Security
BASELINE - Mac iOS 10
BASELINE - Mac iOS 10 Desktop
BASELINE - MS SERVER 2003
BASELINE - MS SERVER 2008 R2
BASELINE - MS SERVER 2012 R2
BASELINE - MS SERVER 2016
BASELINE - MS SERVER DC 2012 R2
BASELINE - MS SQL Server 2012 Database
BASELINE - MS SQL Server 2012 Instance
BASELINE - MS SQL Server 2014 Database
BASELINE - MS SQL Server 2014 Instance
BASELINE - Router Security
BASELINE - Switch Security
BASELINE - Web Server Security
BASELINE - Windows 10
BASELINE - Windows 7

STRATEGY
STRATEGY - Vulnerability Management
STRATEGY - Security Metrics & Reporting

GUIDELINES
GUIDELINE - Major Risk Travel
GUIDELINE - Passphrases
GUIDELINE - Segregation of Duties

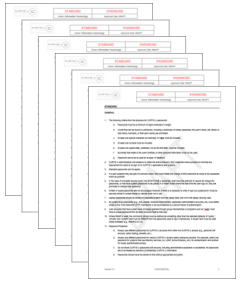
CHARTERS
CHARTER - Change Advisory Board
CHARTER - Digital Security Team
CHARTER - IT Risk Management Team
CHARTER - Security Advisory Team

Executive Committee

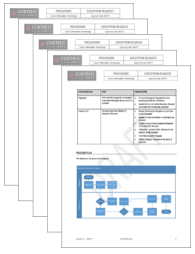
Policy

CIO/CISO

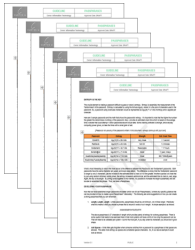
Standards



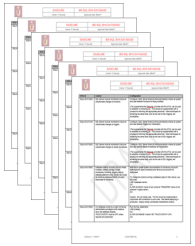
Manager



Procedures



Guidance



Baselines

AUTHORITY

This standard has been created under the authority of [STANDARD AUTHORITY] which maintains the right to ensure that this standard is adhered to.

ENFORCEMENT

Any [ORGANIZATION] employee found to have violated this standard may be subject to disciplinary action including, but not limited to, termination of employment. Any violation of the standard by a temporary worker, contractor or vendor may result in, but not limited to, the termination of their contract or assignment with [ORGANIZATION]. As obligated by provincial and federal laws, [ORGANIZATION] will notify appropriate law enforcement agencies when it appears that any applicable laws have been violated.


MAXIMUM
100

Social Science tells us:

- 20% of compliance → **ANTECEDENT**
- 80% of compliance → **CONSEQUENCE**

CONTROL

If you can't control your peanut butter, you can't expect to control your life."

~ Bill Watterson (Calvin & Hobbes)

- Policy/Standards/Procedures/Guidance/Baselines
- Modularize!
  - Scaled approval process
  - Easier to find things
- Failure to meet Standards must have consequences

SUMMARY

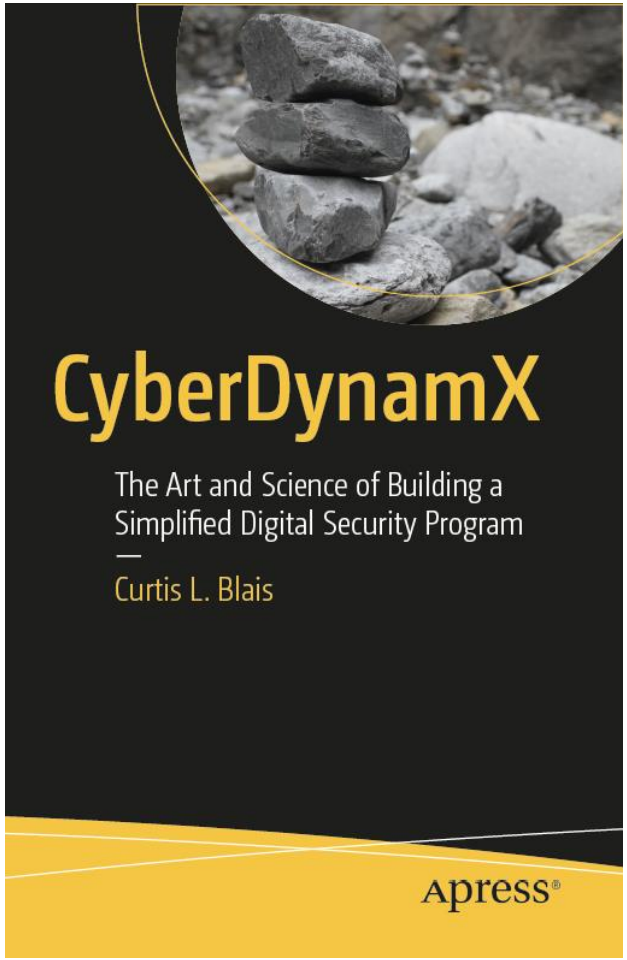
RISK - Common Understanding | Set Tolerance | Defined Actions

CLASS - NOT Records Mgmt. | No Department | Grouping Data

DESIGN - Organization Matters | Op Model for Security (the WHAT)

CONTROL - Modularize (Policy, Standards, etc.)| Consequences

RISK
CLASS
DESIGN
CONTROL



- The Book: **CyberDynamX**
- The Site: cyberdynamx.com

Amazon.ca

Indigo.ca

Thank you!

Curtis L. Blais - Cybera's Shared CISO
MAL, CCNA, CCNP, GCIA, GCFW, WCSP, CISSP, CRISC, CCSK
Harvard Cyber Risk Management
curtis.blais@cybera.ca