3/10/2023

HOW TO CISO:

Communicating in Executive Before the Breach

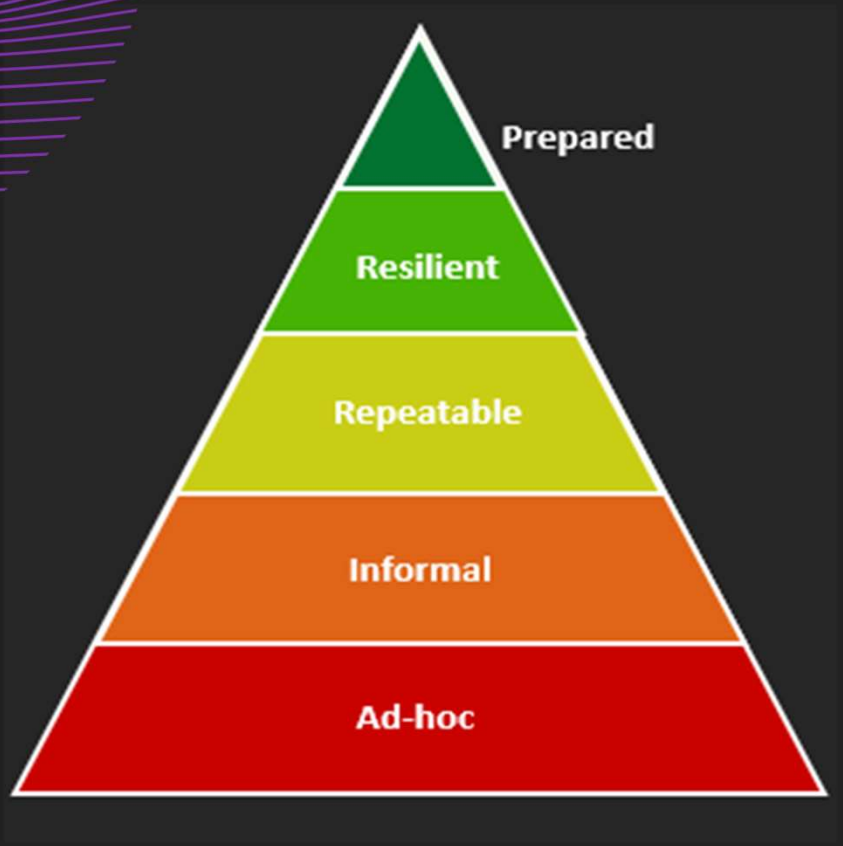
Presented By: Sandy Dunn

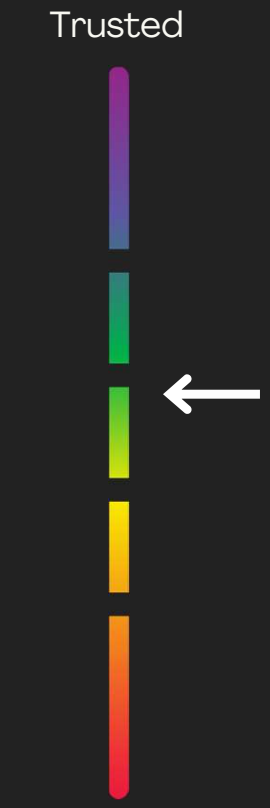
CISO Advisor Shadowscape
Adjunct Professor BSU

TOPICS

- CISO Pyramid of Preparedness
- Strategic Threat Intelligence & Threat Modeling
- Managing an Effective Enterprise Risk Register
- Frameworks & Centralizing Controls & Risk Quantification

CISO PYRAMID OF PREPAREDNESS



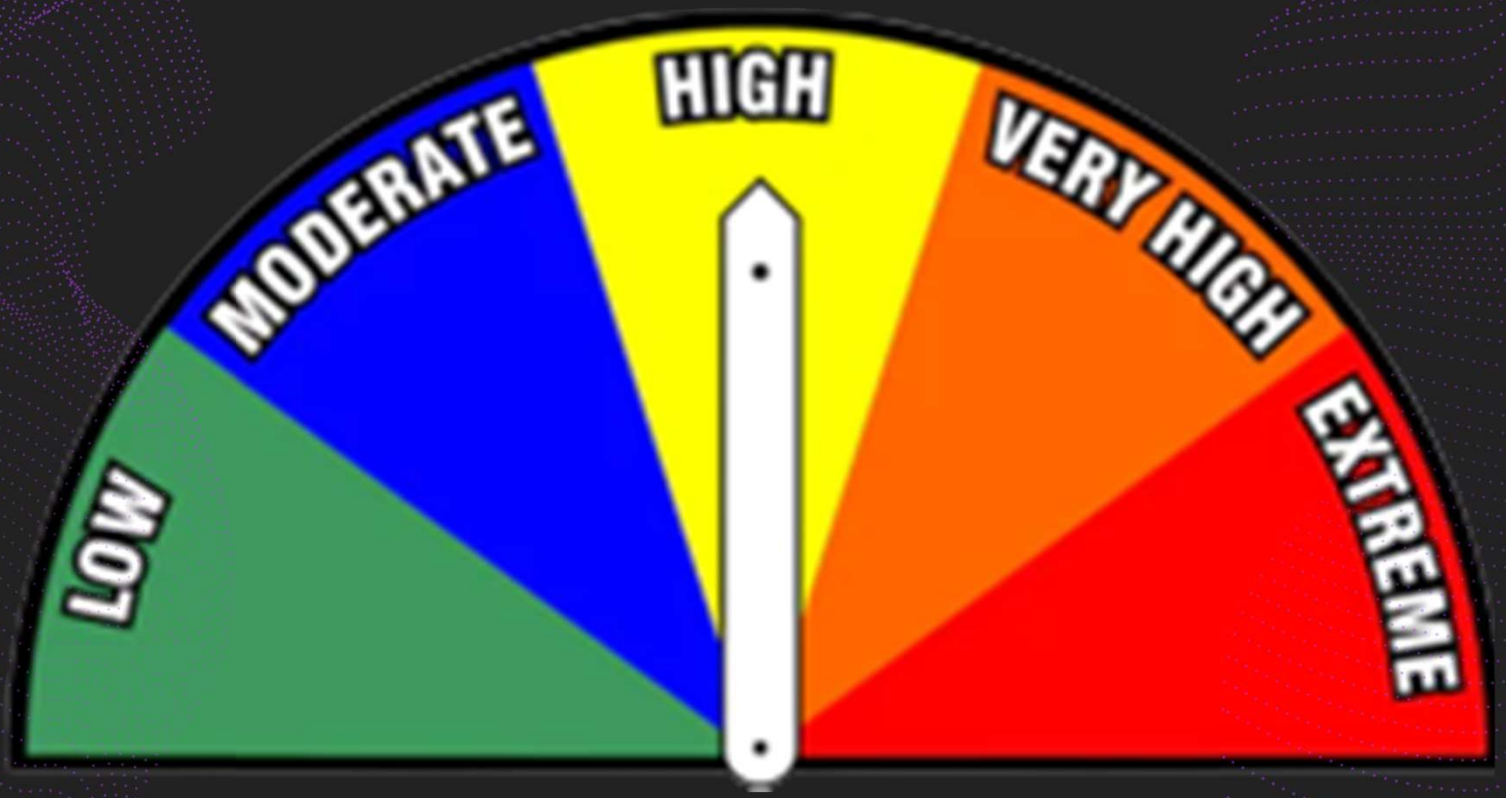



Compliance standards
LastPass has achieved the following third-party security compliances:
SOC2 Type II
SOC3
BSI C5
ISO/IEC 27001:2013
APEC CBPR and PRP Privacy Certification
TRUSTe Enterprise Privacy Certification
SOC II Compliant PCI DSS Certification
ISO 27001 Certification
T-Mobile
mailchimp
LastPass

WHY ?


S
STRENGTH
W
WEAKNESS
O
OPPORTUNITY
T
THREAT
law
MISCOMMUNICATION

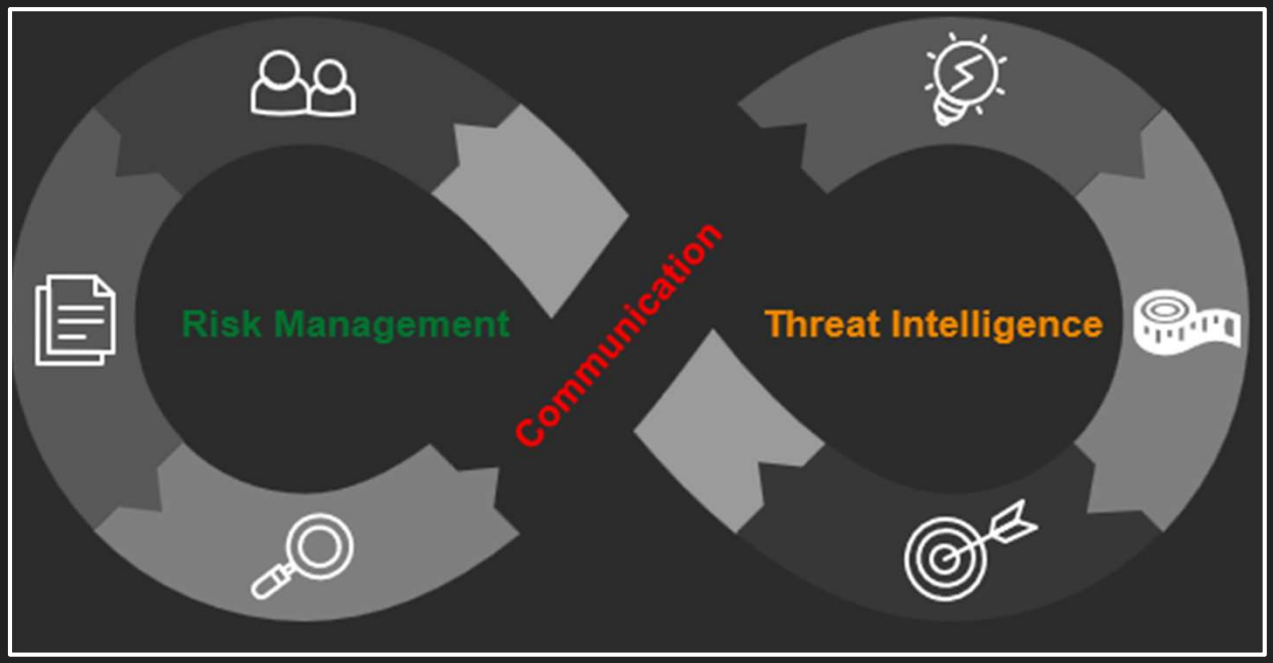
FIRE DANGER TODAY



CISO PYRAMID OF PREPAREDNESS

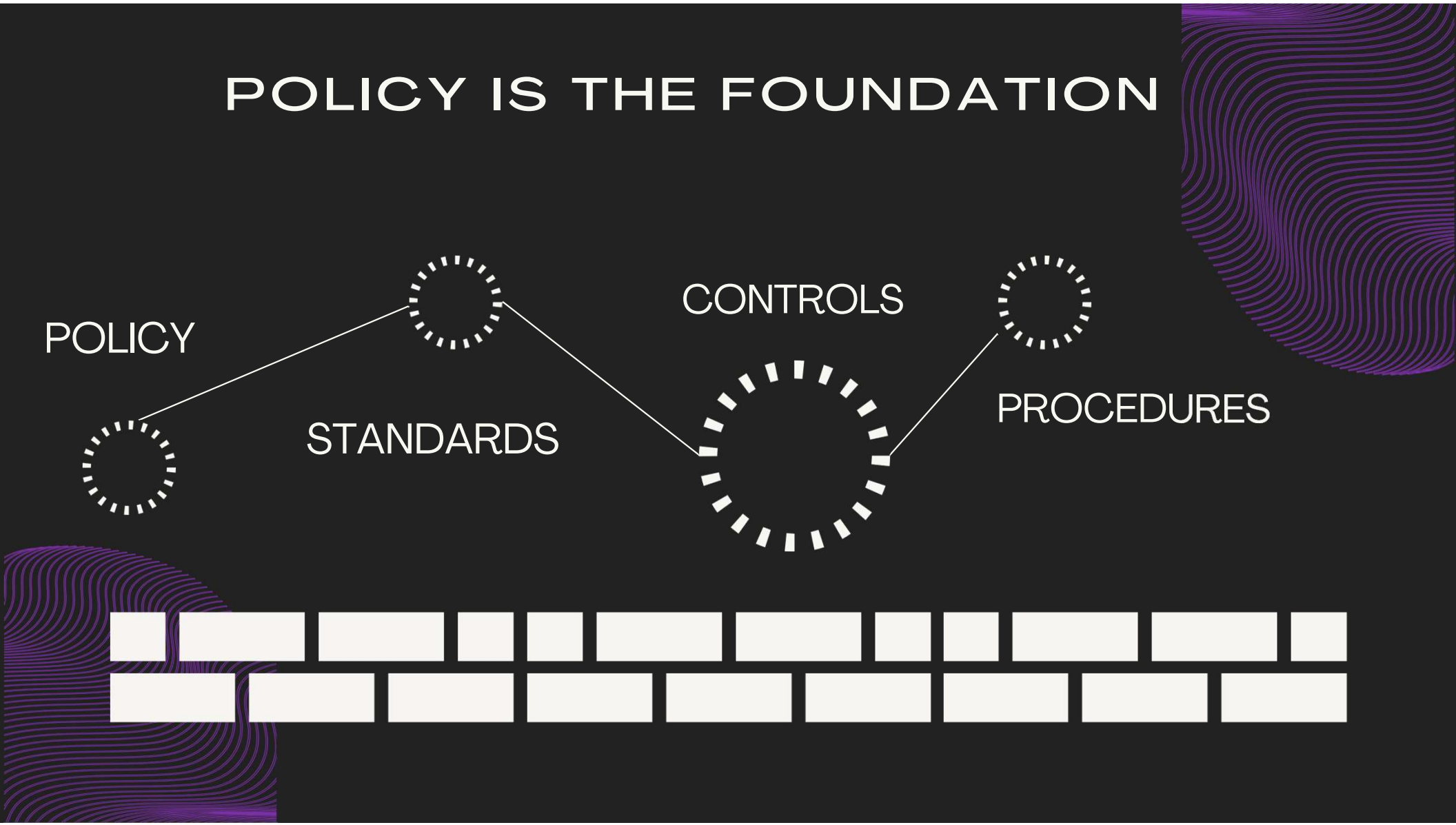
Maturity	Ad-hoc	informal	NEGLIGENCE	Repeatable	Resilient	Prepared
Efficient	0 %	10 %		30 %	60 %	100 %
Strategic Threat Intelligence		Patching based on urgent exploit		Threat model / IOC	Threat reports	PRI drive action
Risk Management / Enterprise Risk Register	• IT Risk register • Potentially financially catastrophic	• Enterprise Risk Register but poor categorization • Potentially large impact to annual revenue goals & target growth		• Rolled into groups in risk register • Incident potentially impacts revenue goals	• KRI measured • Cybersecurity lead • Security potentially overly or under invested	• Metrics, threats, in financial risk • Security investment optimized
Attack surface management		TPRM questionnaires	NEGLIGENCE	Comprehensive scanning	All classes of assets defined & monitored	Strategic threat intelligence requirements tracked
Policy Standards Procedures		Policy for compliance		Policy used to establish standards & procedures	Standards & procedures follow policy	Policy, standards, & procedures embedded
Frameworks		Misused framework		Appropriate use of frameworks	Frameworks aligned to purpose	Effectively used frameworks
Controls	• Ad-hoc controls	Controls not centralized		Standard list of controls	Comprehensive & active testing	Continuous control assessment

STRATEGIC THREAT INTELLIGENCE



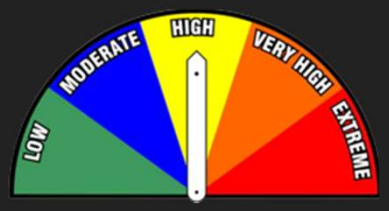
THREAT MODELING

POLICY IS THE FOUNDATION

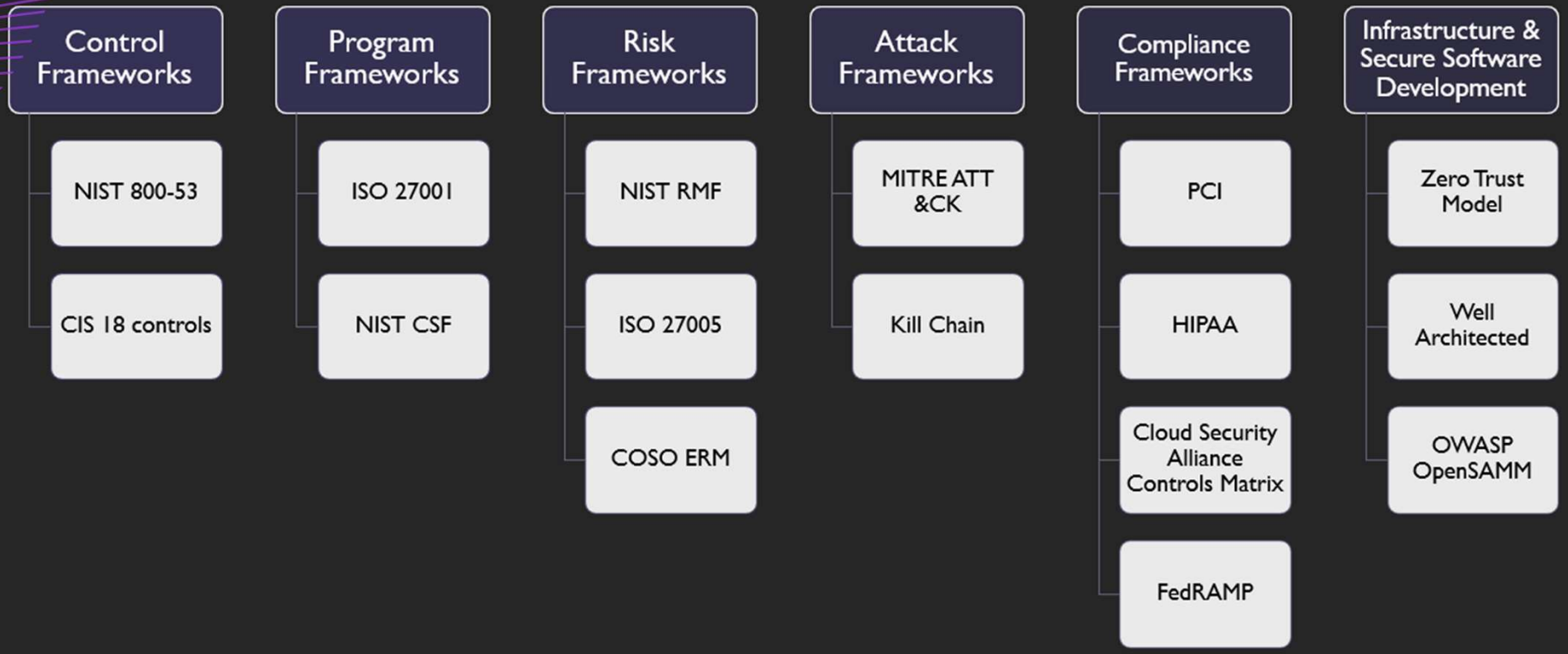


ENTERPRISE RISK REGISTER

NIST IR 8286
Risk aggregation
Identify "adversaries" & Threats



FRAMEWORKS & CONTROLS



THREAT & RISK QUANTIFICATION

Threat			Likelihood			Impact			
5	Very High	80 -100 %	5	Very High	80 -100 %	5	Very High	$10,000,000	80 -100 %
4	High	60 -80 %	4	High	60 -80 %	4	High	$5,000,000	60 -80 %
3	Moderate	40 - 60%	3	Moderate	40 - 60%	3	Moderate	$1,000,000	40 - 60%
2	Low	20 -40 %	2	Low	20 -40 %	2	Low	$500,000	20 -40 %
1	Very Low	0 - 20%	1	Very Low	0 - 20%	1	Very Low	$250,000	0 - 20%

Threat	Likelihood	High	Impact
.9	.7	63 %	$5,000,000

SUMMARY

Use the CISO Pyramid of Progress is a resource to think about your program across the business

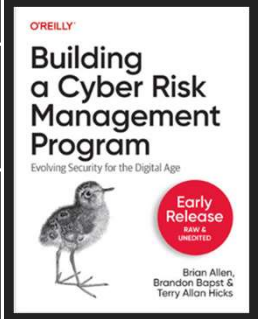
Threat informed risk management *

The Enterprise Risk Register is the barometer for the organization

Operationalize Policy, Standards, frameworks, and controls for a Resilient Digital Transformation Bits factory

RESOURCES

World Economic Forum “Advancing Cyber Resilience Principles and Tools for Boards”	https://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf
NIST IR 8286 Integrating Cybersecurity and Enterprise Risk Management Series	https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf
Security Controls Framework	https://securecontrolsframework.com/
Building a Cyber Risk Management Program	https://learning.oreilly.com/library/view/building-a-cyber/9781098147785/
Threat modeling	https://www.simplilearn.com/what-is-threat-modeling-article
Risk quantification	https://www.fairinstitute.org/blog/https/www.fairinstitute.org/blog/jack-jones-new-edition-cyber-risk-quantification-buyers-guide
Red hat template for Strategic Threat Intelligence & Tracking	**https://github.com/redhat-infosec/priority-intelligence-requirements-devt**



RESOURCES

Unit42 ATOMS by country & type of business	https://unit42.paloaltonetworks.com/atoms/
FISMAC video & educational material	https://fismacs.com/
Jakub Kaluzny OWASP Dublin DevSecOps efficient threat modeling & risk	https://www.youtube.com/watch?v=vk-n4mQMN4A&t=941s
OWASP Risk Rating	https://www.owasp-risk-rating.com/ https://medium.com/geekculture/owasp-risk-calculator-7a8ef11e2477
Summary Stanley McCrystal, “Team of Teams”	https://www.thrivestreetadvisors.com/leadership-library/team-of-teams
Cyber Defense Matrix	https://cyberdefensematrix.com/