

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



Trusted



Not Trusted

A vertical bar with a color gradient from purple at the top to red at the bottom, representing a trust scale. The word "Trusted" is at the top and "Not Trusted" is at the bottom.





Compliance standards

LastPass has achieved the following third-party security compliances:

- SOC2 Type II
- SOC3
- BSI CS
- ISO/IEC 27001:2013
- APEC CEPR and PRP Privacy Certification
- TRUSTe Enterprise Privacy Certification

TRUSTe Certified Privacy Technology




SOC II Compliant PCI DSS Certification

Mailchimp credit card processing service uses security measures to protect your information both during the transaction and after it is complete. The service is certified as compliant with card association security initiatives including the Payment Card Industry Security and Compliance (PCI) Requirements v3.0 Data Protection Program (DPP) and Payment Card Industry Security and Compliance (PCI) Standard version 3.0.2 in public.

We provide our SOC II Report upon request. Please visit the Request Report page under our website's privacy page.

Request Report

ISO 27001 Certification

The International Organization for Standardization (ISO) Standard 27001:2005 is an information security standard that addresses official sites, development systems, support systems, and data centers and security managers. These certifications can be found on our public and open source customer public transparency pages.

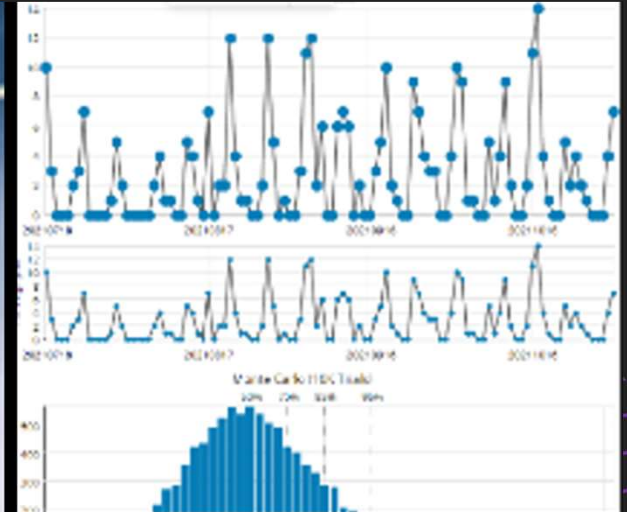
Mailchimp ISO certification





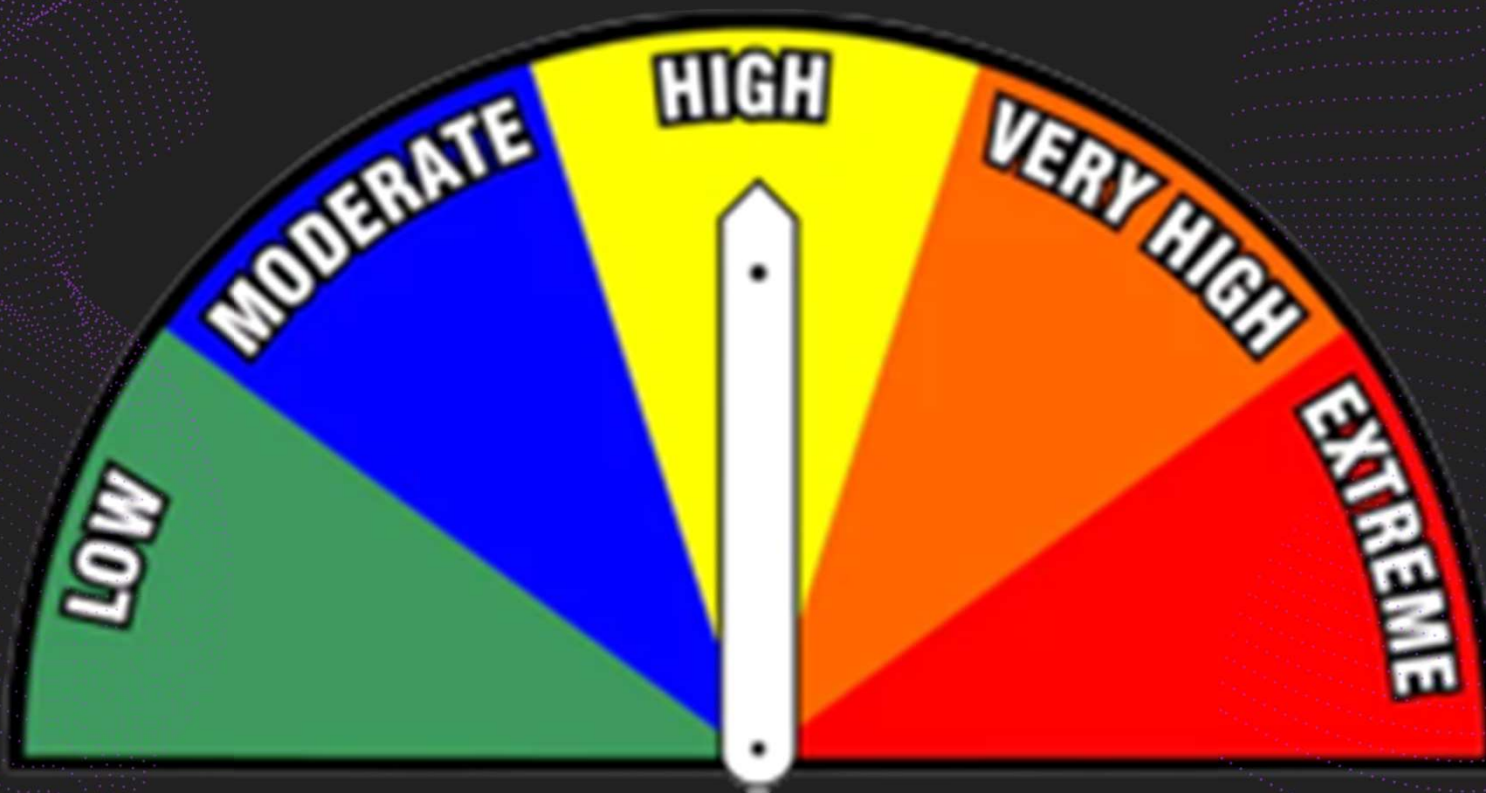
WHY ?





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	<ul style="list-style-type: none"> IT Risk register Potentially financially catastrophic 	<ul style="list-style-type: none"> Enterprise Risk Register but poor categorization Potentially large impact to annual revenue goals & target growth 	NEGLIGENCE	<ul style="list-style-type: none"> Rolled into groups in risk register Incident potentially impacts revenue goals 	<ul style="list-style-type: none"> KRI measured Cybersecurity lead Security potentially overly or under invested 	<ul style="list-style-type: none"> Metrics, threats, in financial risk Security investment optimized
Attack surface management		TPRM questionnaires		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	<ul style="list-style-type: none"> Ad-hoc controls 	Controls not centralized		Standard list of controls	Comprehensive & active testing	Continuous control assessment



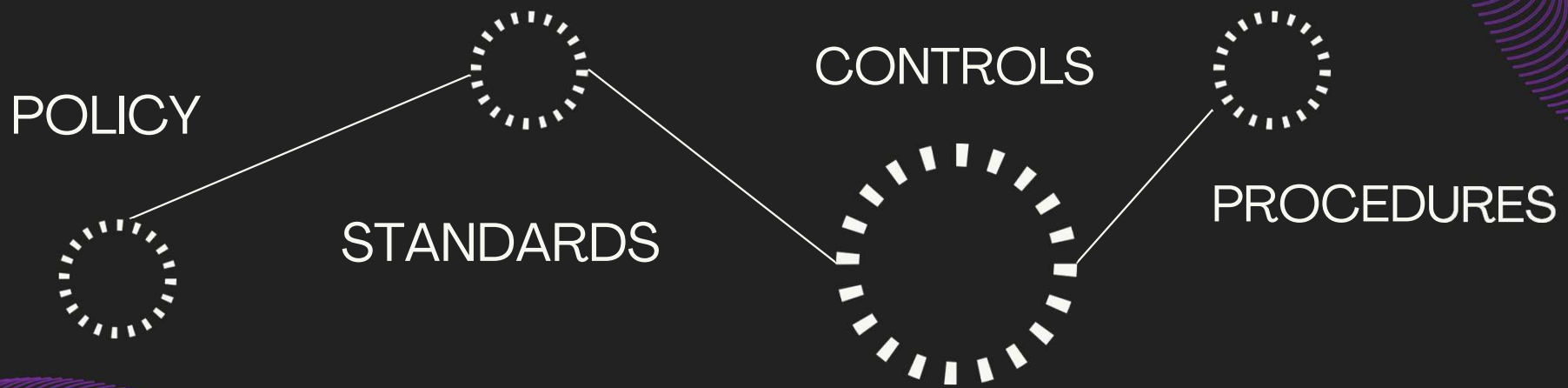
STRATEGIC THREAT INTELLIGENCE



THREAT MODELING



POLICY IS THE FOUNDATION

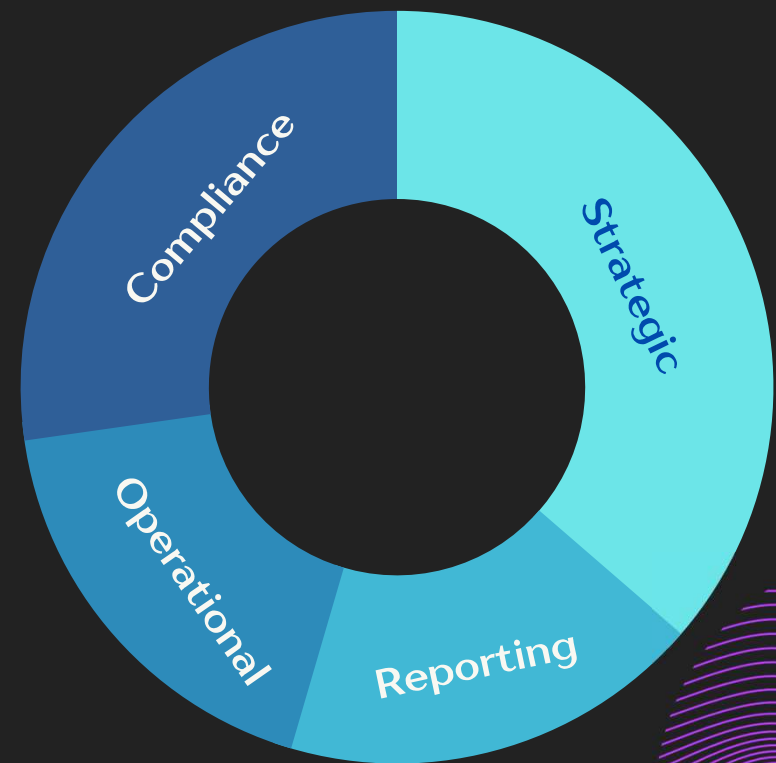
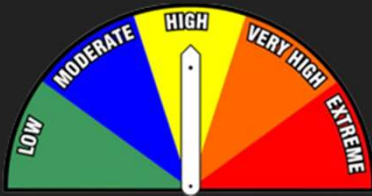


ENTERPRISE RISK REGISTER

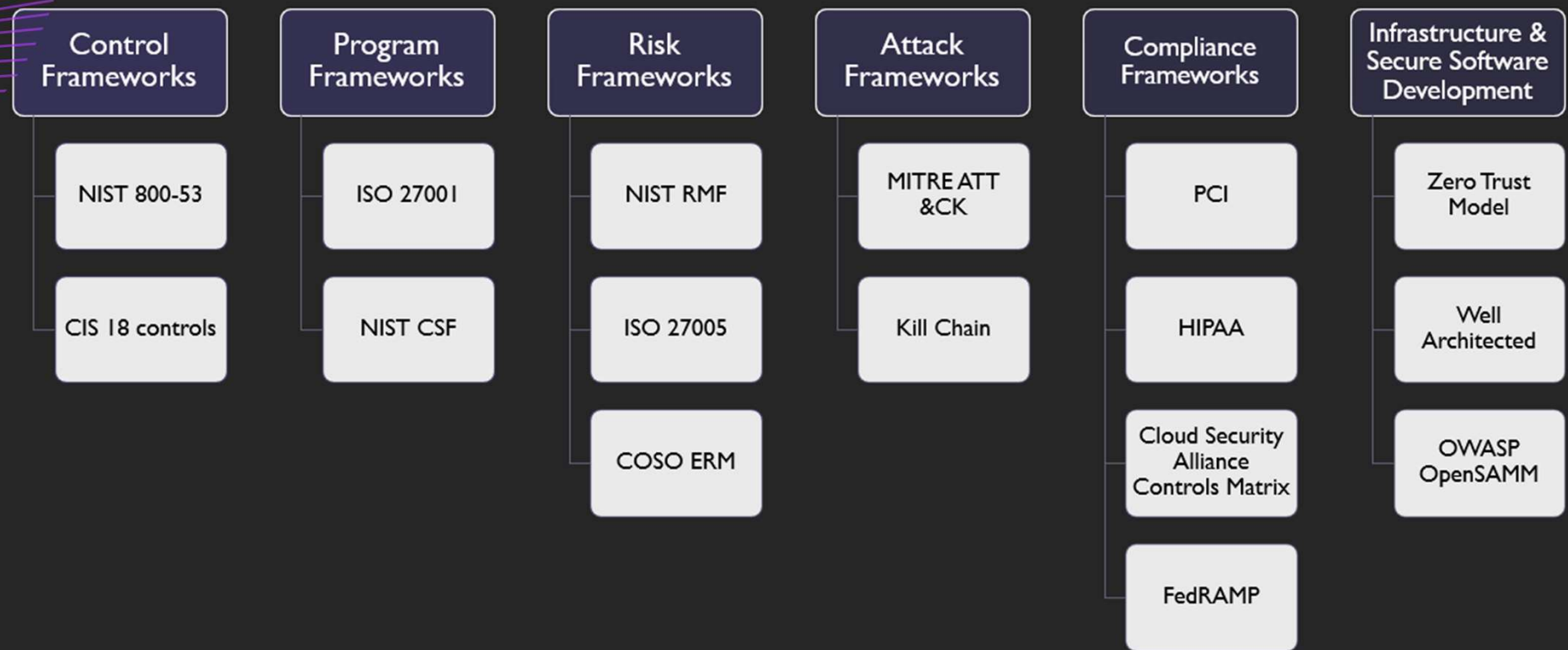
NIST IR 8286

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

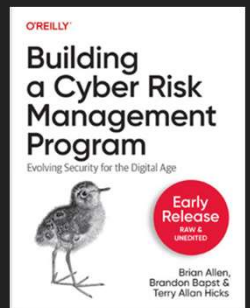
Threat informed risk management *

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/