



MANAGING FINANCIAL CYBERSECURITY  
COUNTERING THE EMERGING THREATS



HANLON  
FINANCIAL SYSTEMS  
CENTER



# May 30, 2018 Conference

©2018 FinCyberSec – All Rights Reserved

[www.FinCyberSec.org](http://www.FinCyberSec.org)



# The Professional Practice of Cybersecurity Risk Management

FinCyberSec 2018

Jennifer Bayuk

May 30, 2018

You can't predict the next attack.

But you CAN  
*manage*  
Cybersecurity Risk!



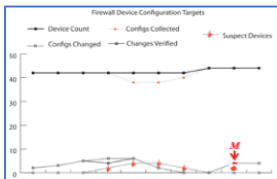
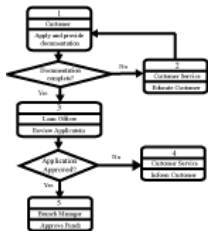
# State of the Practice

Existing Approach:	Cybersecurity Risk Assessment tools are prolific. They focus on well-defined subsets of the cybersecurity landscape and encompass a wide variety of disparate evaluation criteria, such as control gaps, maturity levels, and tiers.
Problem Statement:	Most individual cybersecurity assessors, even those in large firms, make sense of the disparity by creating custom spreadsheets in which they reduce cybersecurity assessment materials to sets of individual questions/requirements and structure assessment results into actionable sets of issues.
Vision:	A new global framework for professional practice of cybersecurity risk management, one that takes advantage of existing assessment guidelines, but normalizes assessment results to continuously improve cybersecurity risk assessment capability.

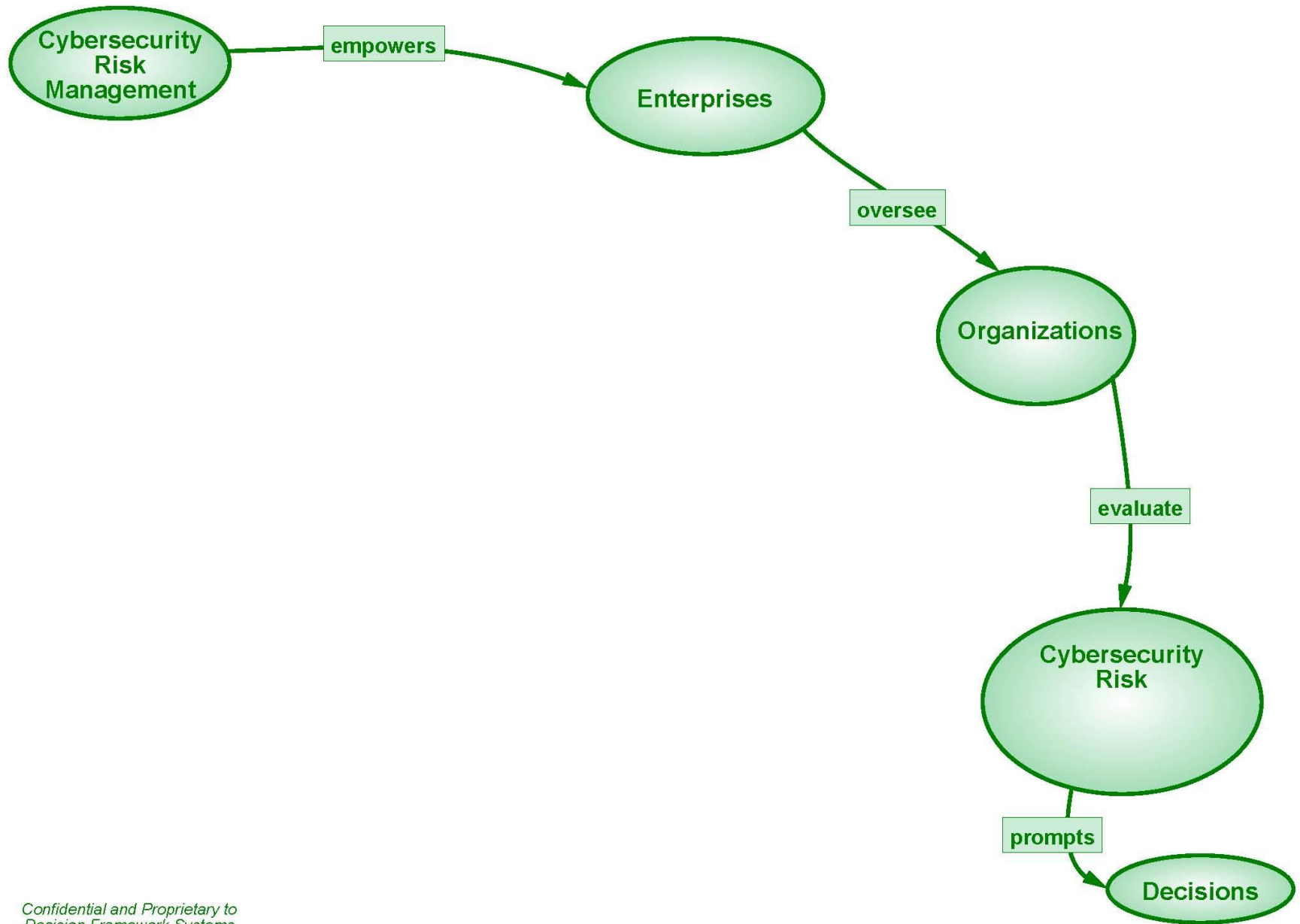


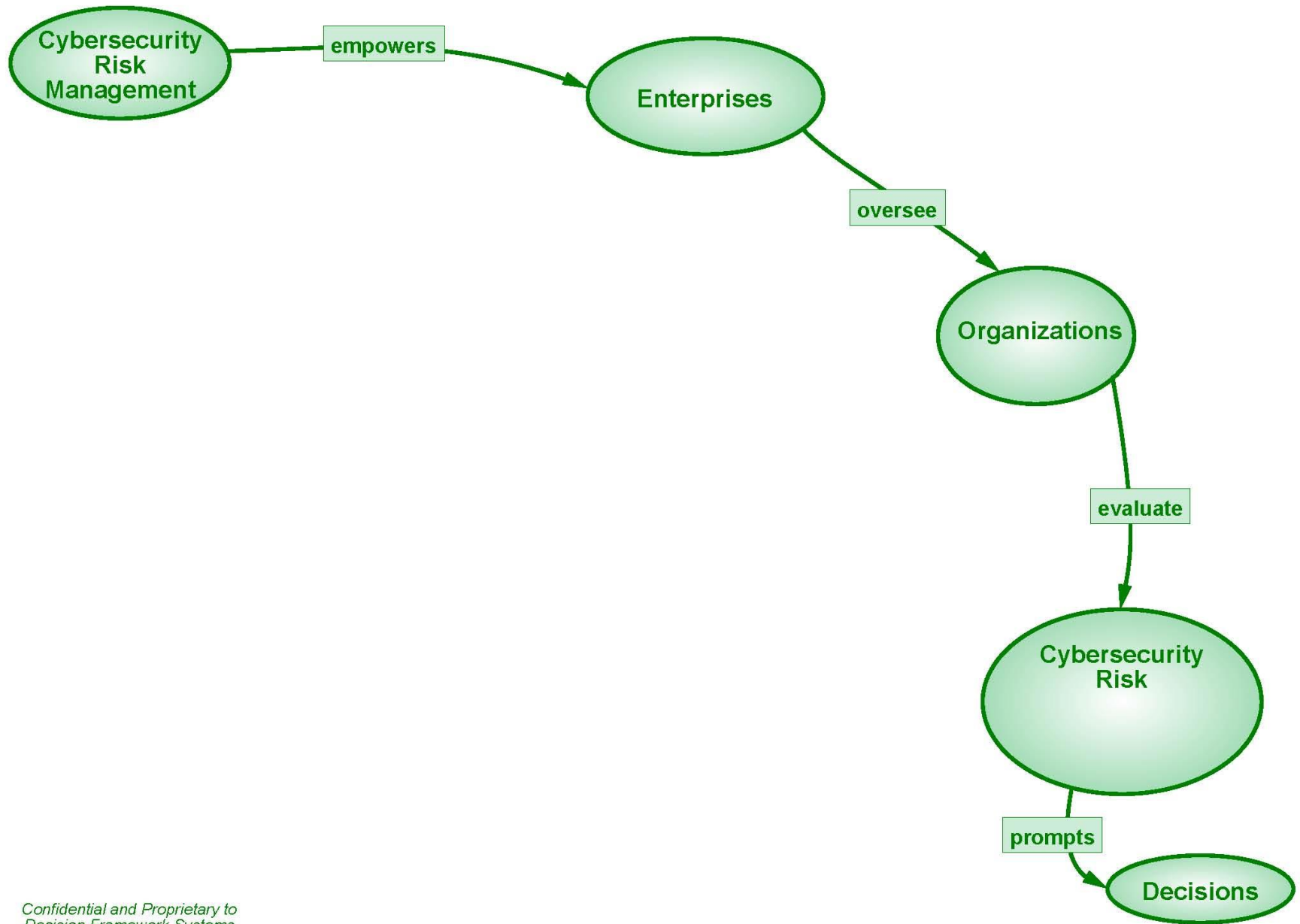
## A small, four-armed drone is shown in flight against a bright, hazy sky at sunset or sunrise. The drone is positioned in the upper center of the frame. Below it, the dark silhouettes of a city skyline are visible, including several tall buildings. The overall scene suggests a high-altitude aerial view of an urban area.

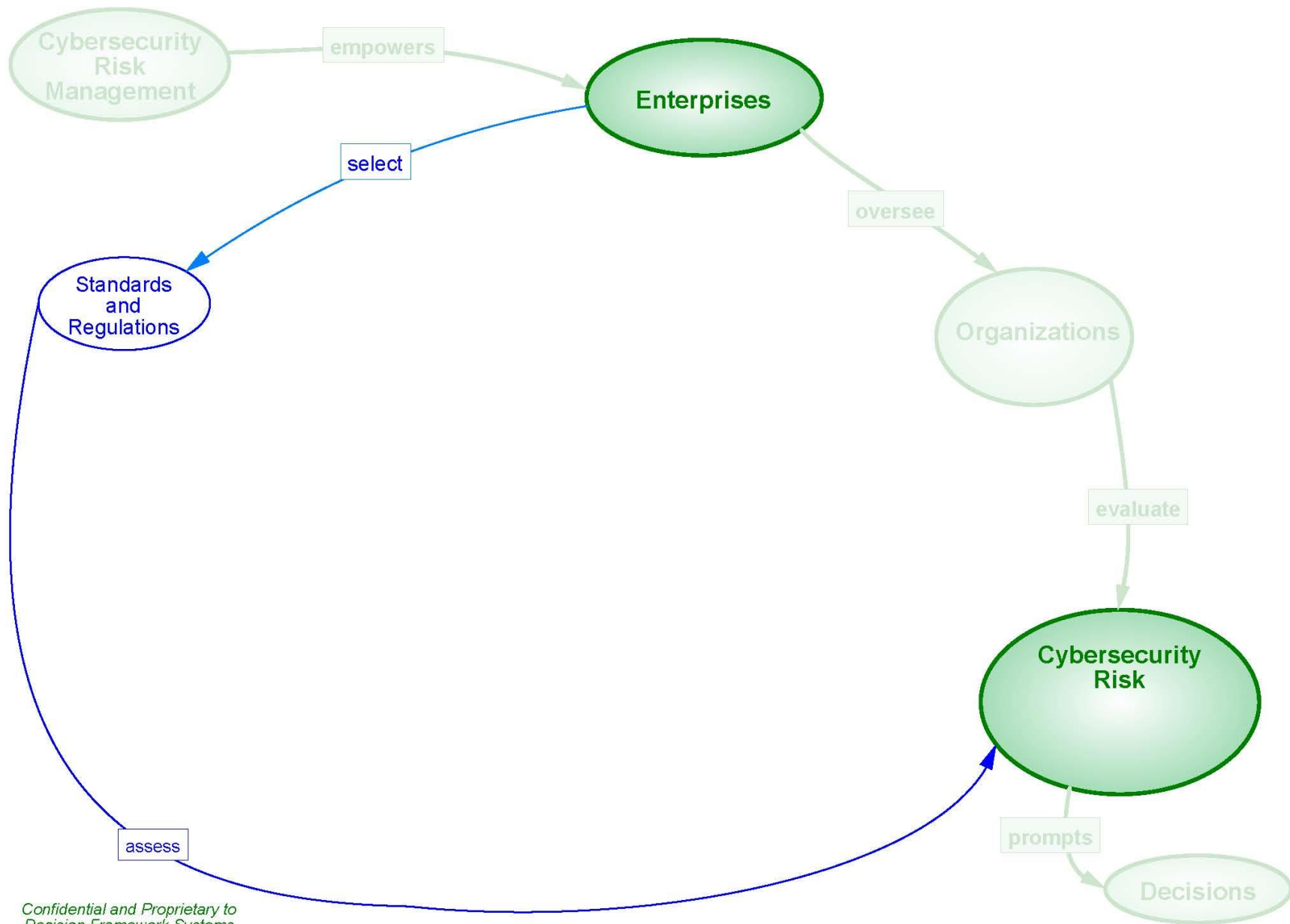
Topic	Author	Section	Publication Source	Page No.	Comments
1 Cyber Risk Management & Oversight	Government	Oversight Executive	Oversees operations of the Department and is responsible for the Department's cybersecurity strategy, including the Department's cybersecurity policy, strategy, and program. The Director is responsible for implementing and maintaining the Department's security and business continuity programs. (FTEC Information Security Review, page 30)	10	Correlate Policy with Implementation
2 Cyber Risk Management & Oversight	Government	Oversight Executive	Oversees the Department's information security risks and is responsible for the Department's information security policy, strategy, and program. The Director is responsible for implementing and maintaining the Department's security and business continuity programs. (FTEC Information Security Review, page 30)	10	There is a number of references to the Department's information security management strategy.
3 Cyber Risk Management & Oversight	Government	Oversight Executive	Management provides a written report to the oversight committee on the Department's information security and business continuity programs. The report includes the Department's information security and business continuity programs, the Department's information security and business continuity programs, and the Department's information security and business continuity programs. (FTEC Information Security Review, page 30)	10	The annual reports cover cybersecurity and business continuity, and most detailed reports are available to the public.
4 Cyber Risk Management & Oversight	Government	Oversight Executive	The Department's information security and business continuity programs are reviewed and approved by the oversight committee. The Department's information security and business continuity programs are reviewed and approved by the oversight committee. (FTEC Information Security Review, page 30)	10	Information security is a separate budget line.



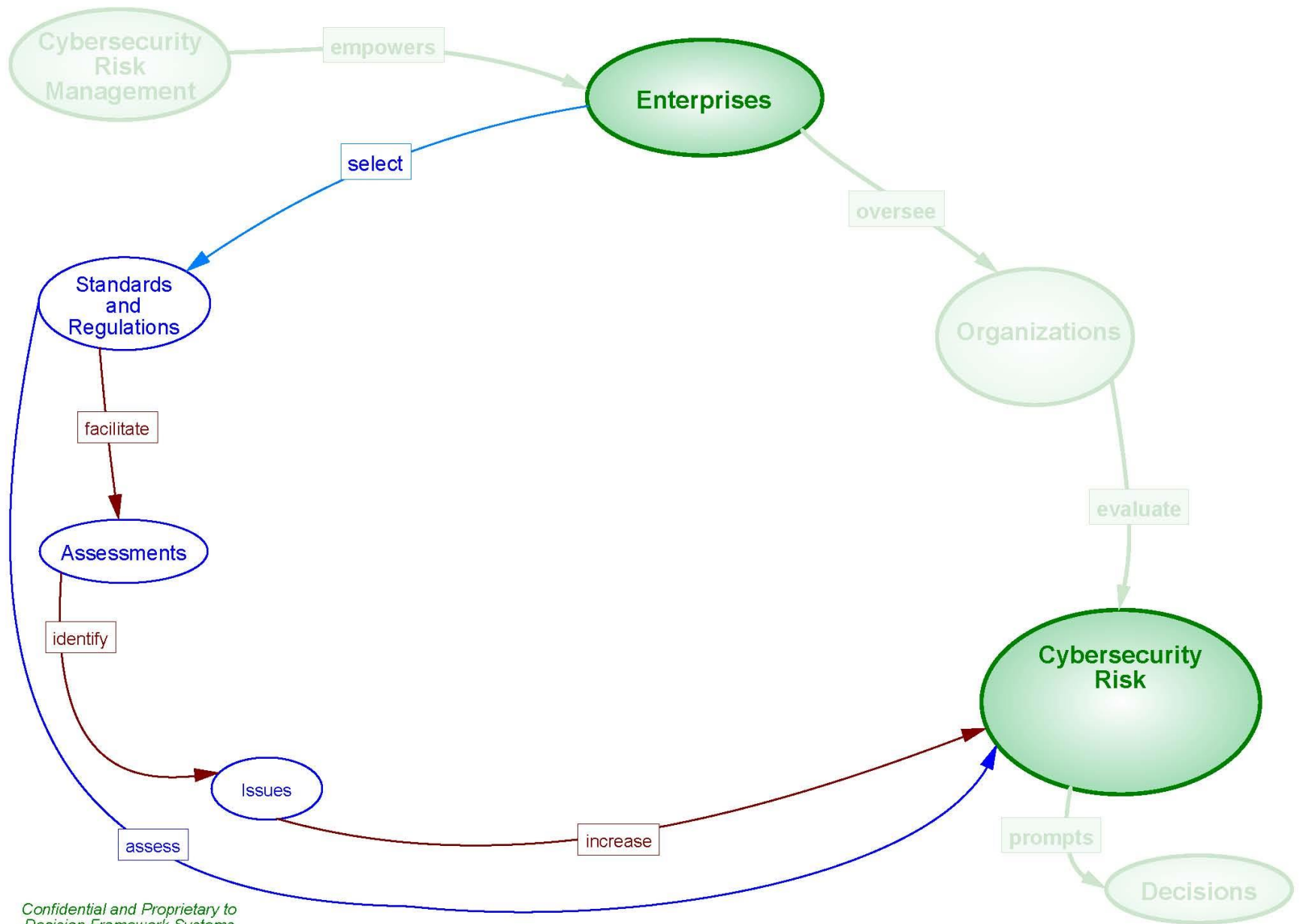
-

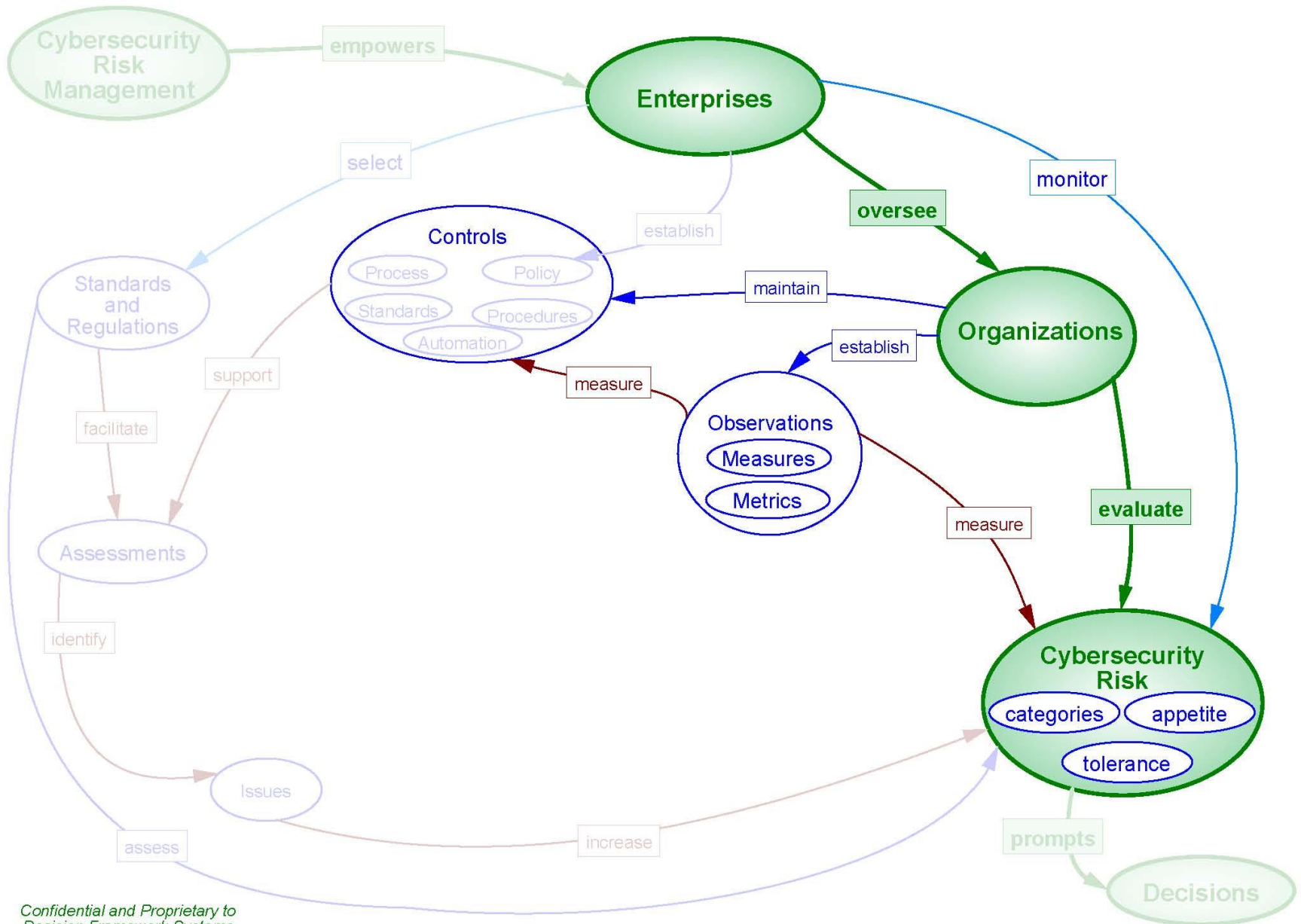


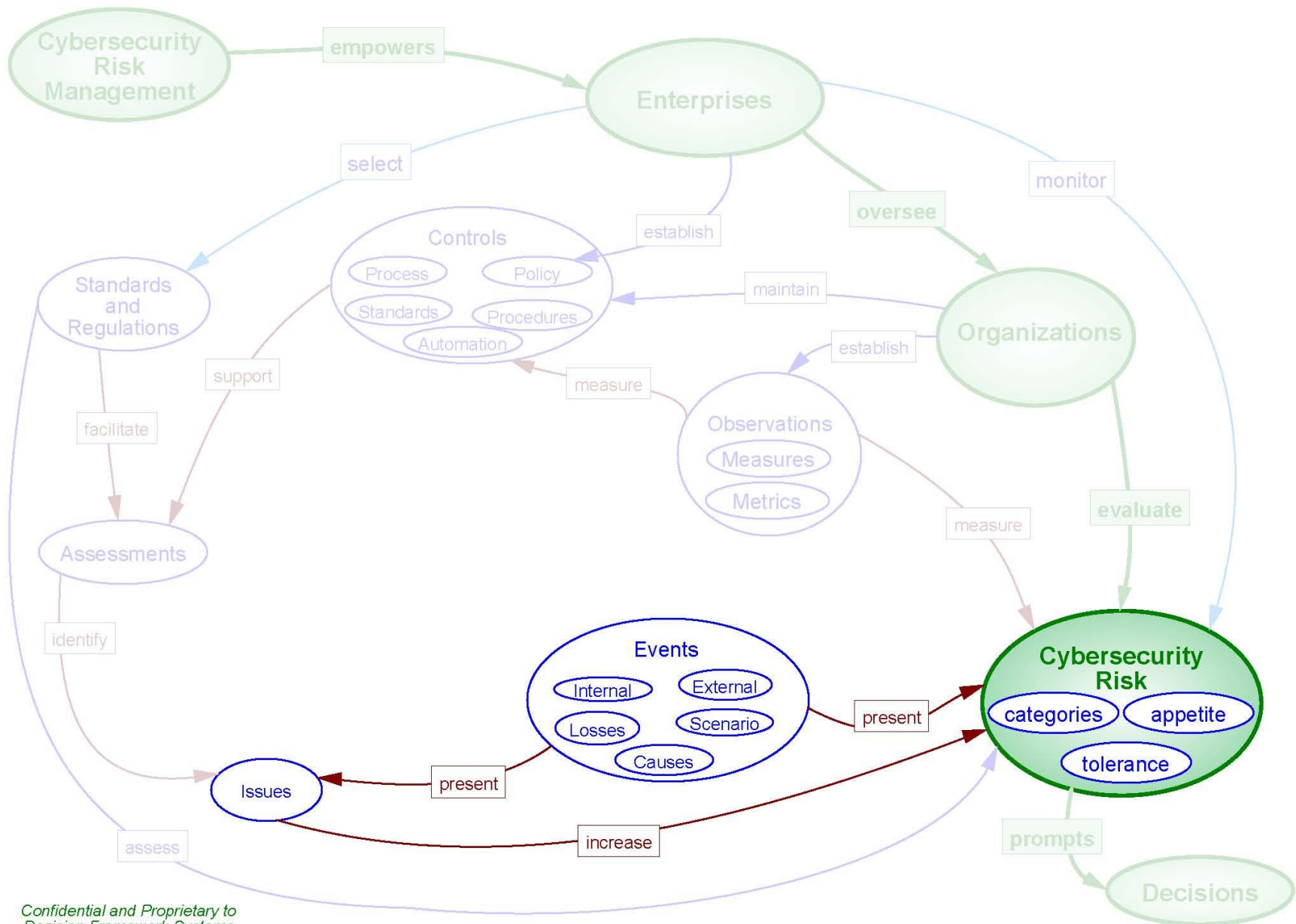


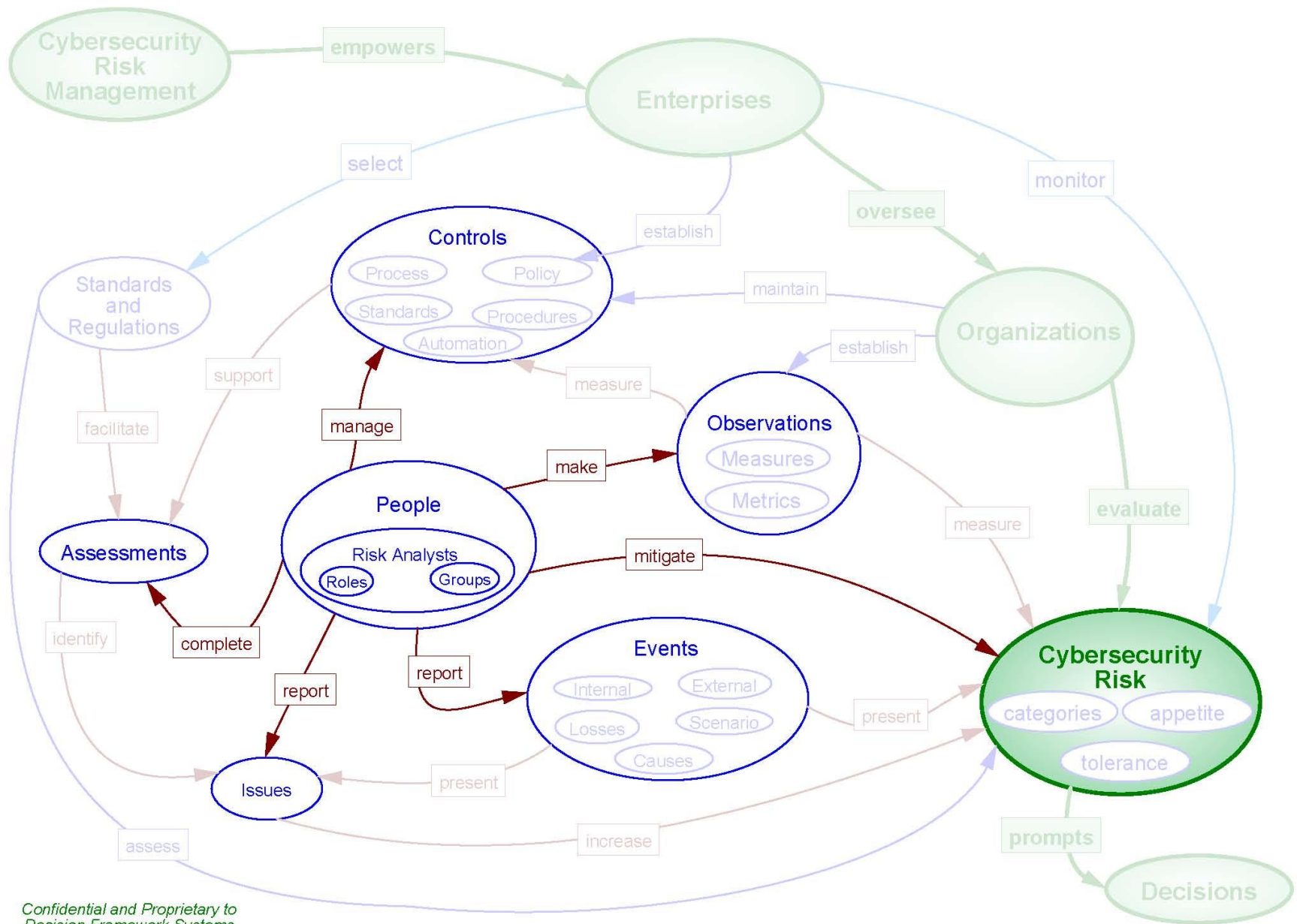


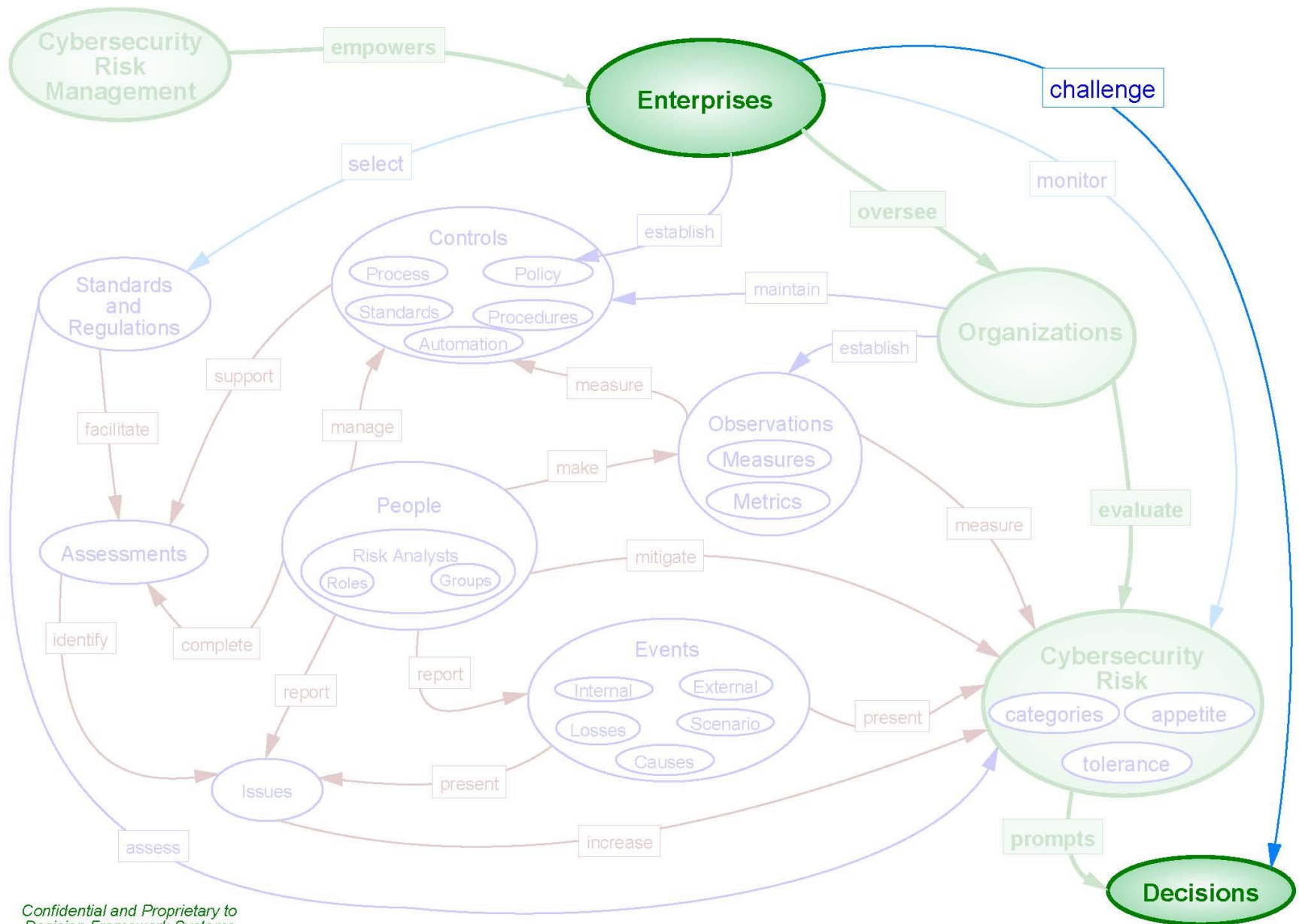




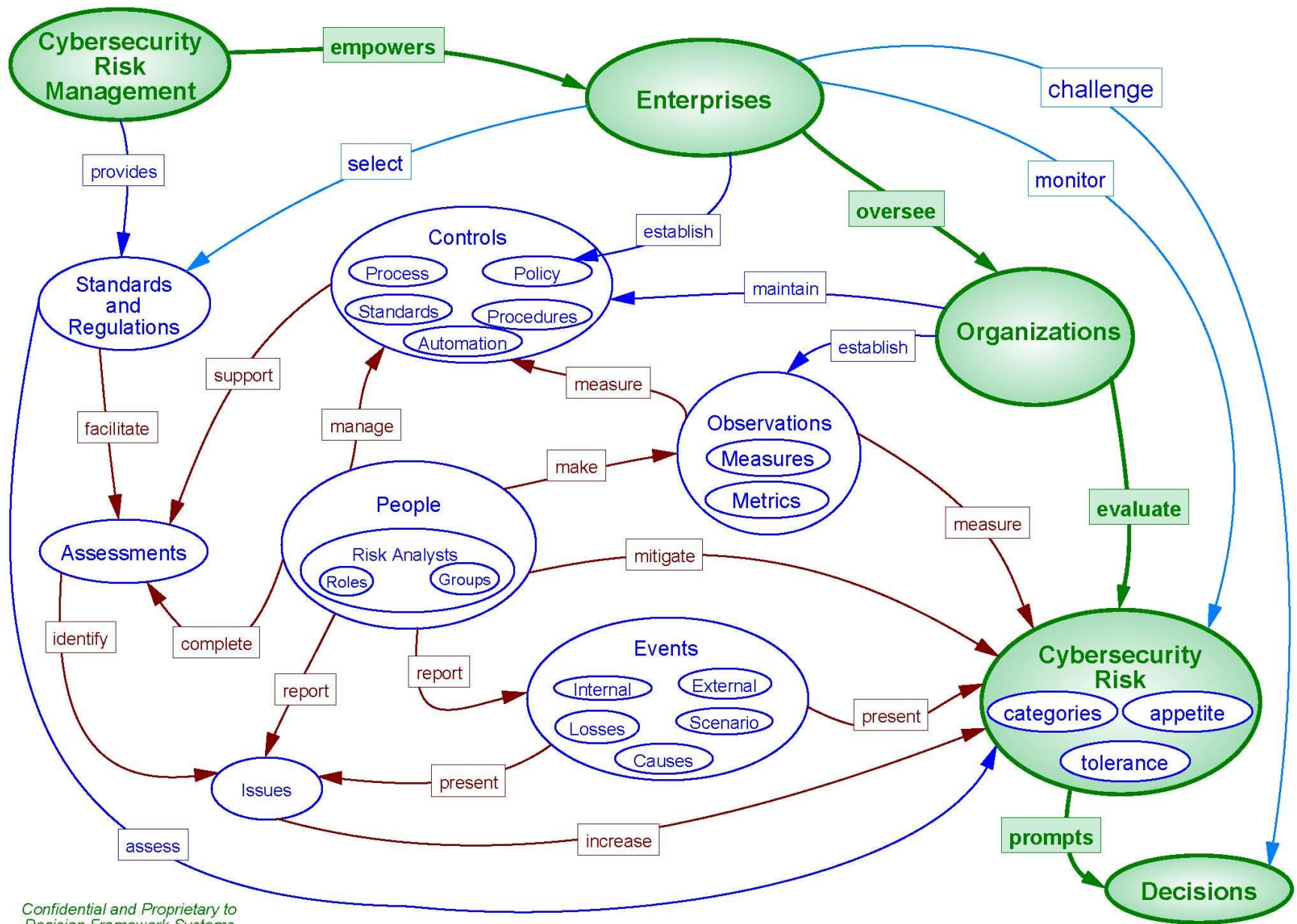




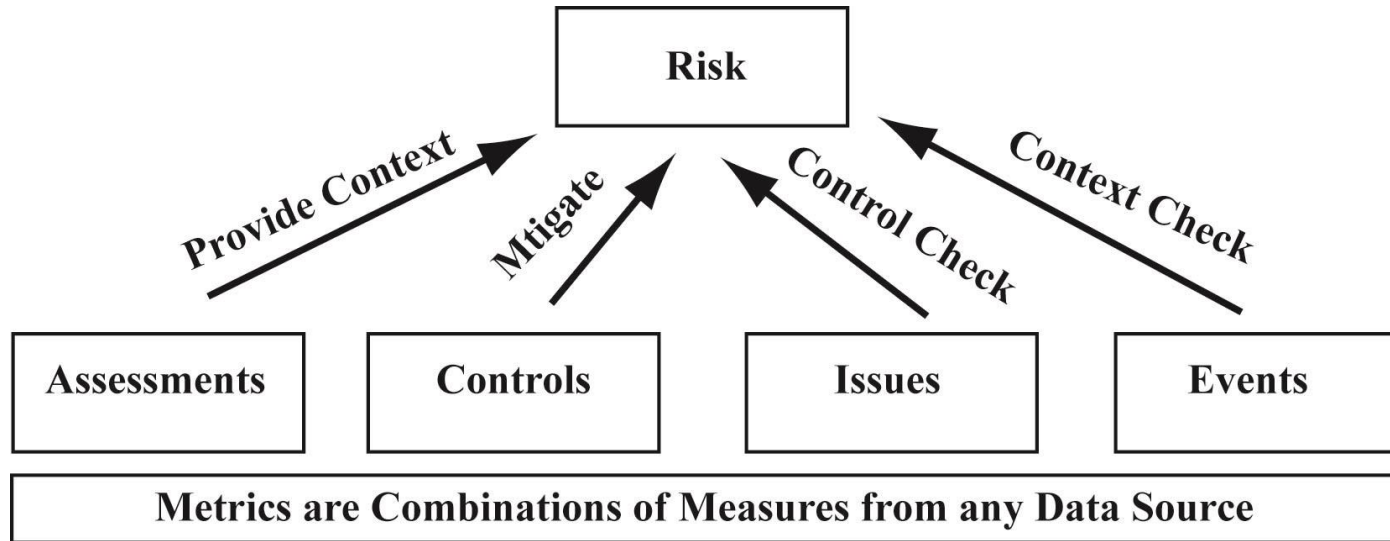








# Quantitative Data Analysis



- Assessments are sets of requirements that are deemed appropriate to apply to an organization. They are guides to risk reduction.
- Controls are relevant to risk in the context of sound Software Architecture and Infrastructure Engineering that demonstrates actual risk mitigation.
- Events and Issues align with risk categories, and can indicate probable new events by category.
- *Risk appetite* is a qualitative description of the amount of risk a firm is willing to accept with respect to a given category of events.
- *Risk tolerance* refers specifically to the boundaries of acceptable variations in performance related to achieving objectives, while risk indicators are measures that help identify changes to the risks themselves.



# Example Approach

FRAMECYBER JLB

Assessment: A000009: WTG SWIFT-CSCF Bayuk (E000001)

Assessments | Workpapers | Issues | Events | Risks | Analysis | Enterprise | Controls | Metrics | People | Profile

Requirement 1.1

Observations

Restrict Internet Access and Protect Critical Systems from ...  
SWIFT Environment Protection

Mandatory for In-house ... Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.

A segregated secure zone safeguards the user's SWIFT infrastructure from compromises and attacks on the broader enterprise and external environments. Control Context: Segmentation between the user's local SWIFT infrastructure and its

Filter List

Reference	Status	Section
1.1	Meets	Restrict Internet Access and Protect Critical Systems from General IT Env...
1.2	ToDo	Restrict Internet Access and Protect Critical Systems from General IT Env...
2.1	ToDo	Reduce Attack Surface and Vulnerabilities
2.2	ToDo	Reduce Attack Surface and Vulnerabilities
2.3	ToDo	Reduce Attack Surface and Vulnerabilities
2.4A	ToDo	Reduce Attack Surface and Vulnerabilities

Confidential

Controls | Events | Issues | Measures | Metrics

FRAMECYBER - Risks

Assessments | Workpapers | Issues | Events | Risks | Analysis | Enterprise | Controls | Metrics | People | Profile

Source: Firm Top Ten Risks (TopTen)

Index: CS-I Name: Harm to integrity

Likelihood: 70

Inherent: High

Residual: Medium

Appetite: The firm has no tolerance for known vulnerabilities in its systems.

Filter List

Source	Index	Na
TopTen	CS	Cybersecurity
TopTen	CS-C	Harm to confidentiality
TopTen	CS-I	Harm to integrity
TopTen	CS-A	Harm to availability
TopTen	Tech	Technology
TopTen	TP	Third Party
TopTen	Ops	Operational
TopTen	Ops-Internal	Internal Events

Confidential

Controls | Events | Issues | Measures | Metrics | Key Metrics | Organization

## Report for Risk: Harm to integrity (CS-I)

Key Risk: Yes

Inherent Risk: High

Residual Risk: Medium

Likelihood: 70%

Controls: TAG-Cyber: Cyber-13: Infrastructure Security  
TAG-Cyber: Cyber-35: Application Security

Metrics: Cyber-KCI-1 - Metric1 Indicator reflects ability of technology to maintain controls.  
Cybersecurity-Infrastructure - Metric2 Indicator reflects security of technology infrastructure.  
Cyber-KCI-2 - Metric3 Indicator reflects ability of technology to appropriately prioritize control implementation.

Issues: BB10: Entitlement to accounts can be compromised via social media sign-on. - Bug bounty program report that web user can see email of customers who post comments on knowledge base page by viewing source. Source: Bug Bounty-10 (FIS)  
I4: SWIFT-CSCF requirement: 1.1-a.2 - Does not meet assessment requirement. Design goals for segregation include, to the fullest extent possible, passwords and other authenticators that are usable inside the secure zone (especially for privileged accounts) are not stored or used in any form (hashed, encrypted, or plaintext) in systems outside of the secure zone. This does not apply to encrypted backup files. Source: Assessment-A000007-1.1-a.2 (WTG)

Events: Internal (WTG): 1 - Wire Transfer Fraud Wire Transfer operator employee used stolen authentication to transfer customer funds to a relative's account

Category: TopTen (CRO): CS - Cybersecurity intentional harm to systems confidentiality, integrity, and availability due to actors with malicious intent

Last Update: 2018-06-27 13:47:22 by Jennifer Bayuk



See <http://www.framecyber.com>



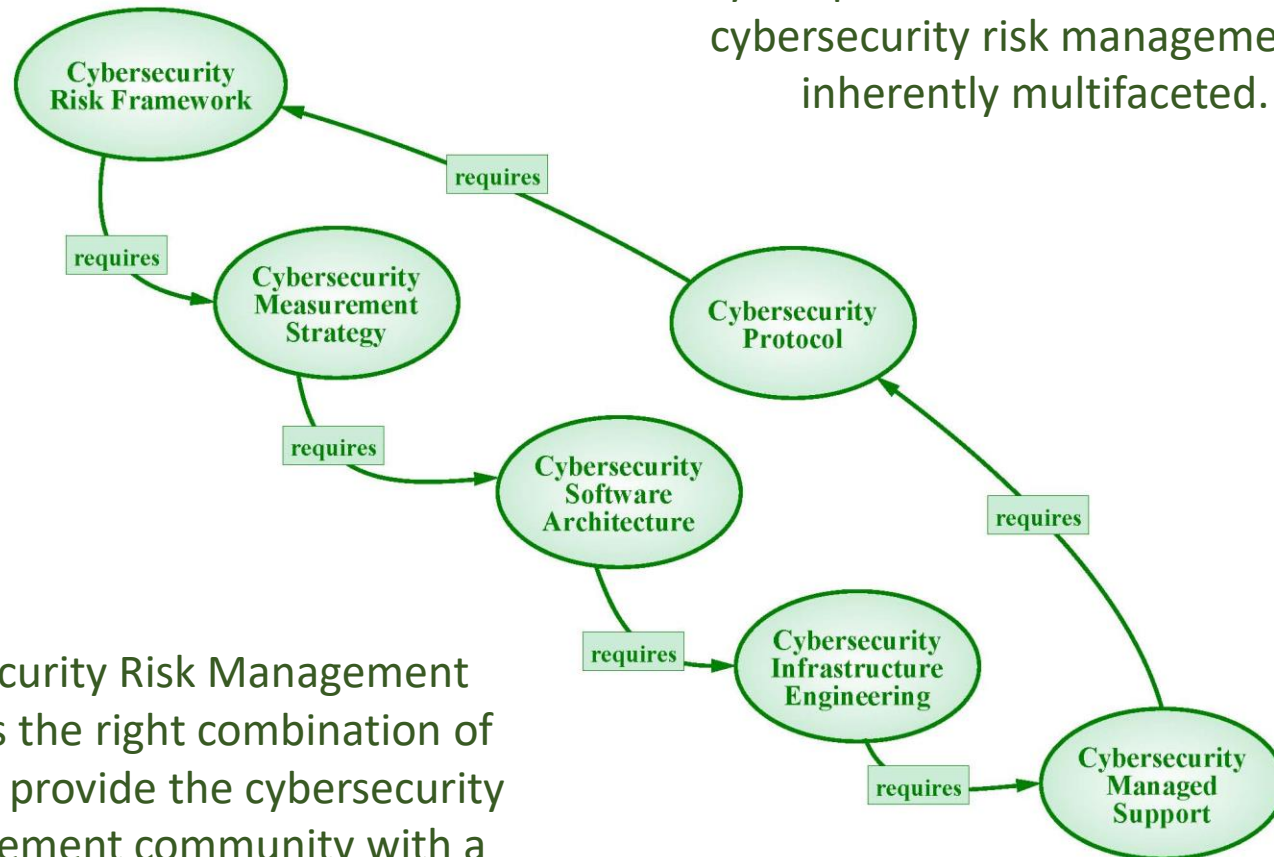
# Qualitative Assumptions

- Expertise in technology measures and metrics are essential to objective observation of controls.
- Risk tolerance measures are always based on expert judgement.
- Events are indisputable evidence (*facts matter*).
- Agreement on issue severity implies tacit agreement on best practice protocol in both risk reduction goals and cybersecurity hygiene ( “*what good looks like*” )
- People and process are as important to measure and monitor as technology.



# Cybersecurity Risk Team Roles and Responsibilities

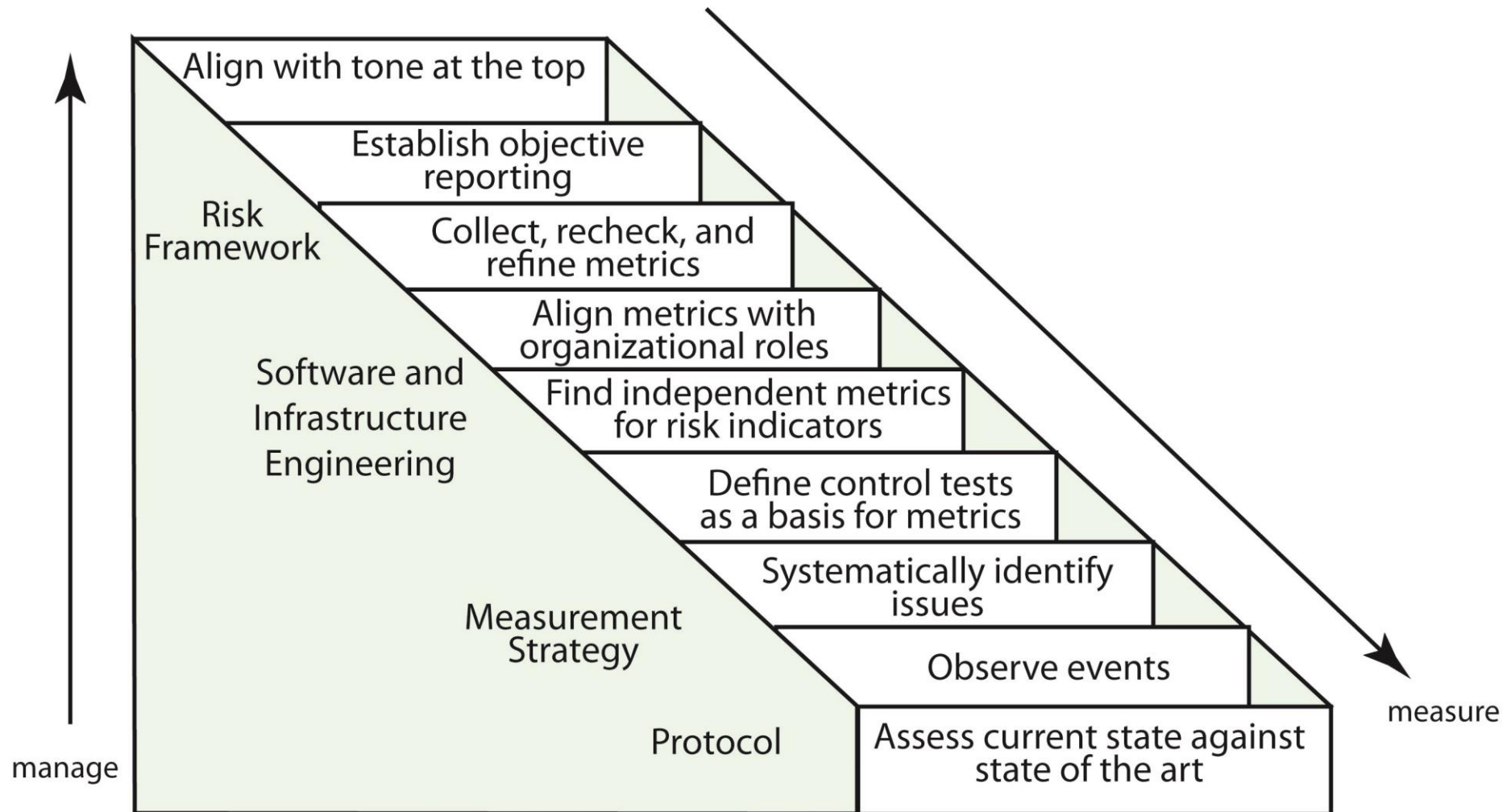
Cyberspace is interconnected, and cybersecurity risk management is inherently multifaceted.



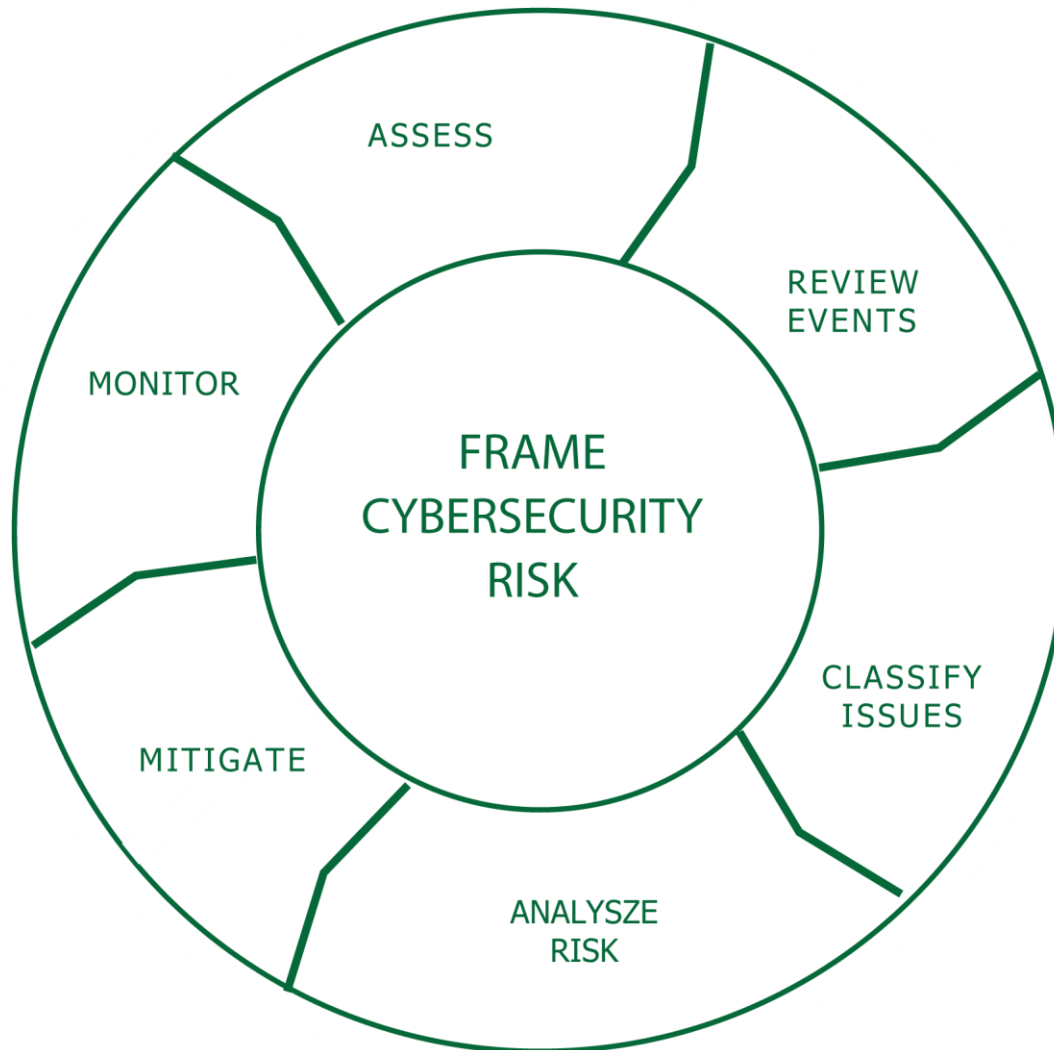
A Cybersecurity Risk Management team needs the right combination of expertise to provide the cybersecurity risk management community with a reliable, repeatable, and maintainable continuous cybersecurity risk assessment framework



# Cybersecurity Framework Build Process



# Cybersecurity Risk Management Cycle



Continuous simultaneous observation of all cycle phases maintains focus on both systemic and emerging risk.



*Questions?*

*Discussion*

*[jennifer@bayuk.com](mailto:jennifer@bayuk.com)*

*[www.framecyber.com](http://www.framecyber.com)*

*973-335-3530*



# Appendix

---



# FFIEC Automated Cybersecurity Assessment Tool Excerpt

Domain	Assessment Factor	Component	Maturity Level	Mapping Number	Declarative Statement	Appendix A Baseline Mapping	FFIEC Declared Mapping to NIST Subcategories	Yes, No, and N/A	Comments
1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	D1.G.Ov.B.1	Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. (FFIEC Information Security Booklet, page 3)	Source: IS.B.3: Financial institutions should implement an ongoing security process and institute appropriate governance for the security function, assigning clear and appropriate roles and responsibilities to the board of directors, management, and employees. Additional reference:1 Information Security and Management Booklets.	<b>ID.GV-4:</b> Governance and risk management processes address cybersecurity risks. (p. 22)  <b>ID.RM-1:</b> Risk management processes are managed and agreed to by organizational stakeholders. (p. 23)	Yes	Corporate Policy holds management accountable.
1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	D1.G.Ov.B.2	Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. (FFIEC Information Security Booklet, page 6)	Source: IS.B.6: Senior management should clearly support all aspects of the information security program... participate in assessing the effect of security issues on the financial institution and its business lines and processes.	There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. (p. 10)	No	There is no evidence of cybersecurity risk discussion in management meetings.
1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	D1.G.Ov.B.3	Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. (FFIEC Information Security Booklet, page 5)	Source: IS.B.5: The board should approve written information security policies and the written report on the effectiveness of the information security program at least annually. * Information Security, Management	<b>ID.GV-4:</b> Governance and risk management processes address cybersecurity risks. (p. 22)	Yes	The annual reports cover cybersecurity and business continuity, and more detailed versions are available to the Board.
1: Cyber Risk Management & Oversight	1: Governance	1: Oversight	Baseline	D1.G.Ov.B.4	The budgeting process includes information security related expenses and tools. (FFIEC E-Banking Booklet, page 20)	Source: EB.B.20: Financial institutions should base any decision to implement e-banking products and services on a thorough analysis of the costs and benefits associated with such action. The individuals conducting the cost-benefit analysis should clearly understand the risks associated with e-banking so that cost considerations fully incorporate appropriate risk mitigation controls.  EB.WP.2.2: Determine the adequacy of board and management oversight of e-banking activities with respect to strategy,	None	Yes	Information security is a separate budget item.





# Target Metric with Monitor Overlay

Daily Measure W:

The number of firewall devices in operation.

Daily Measure X:

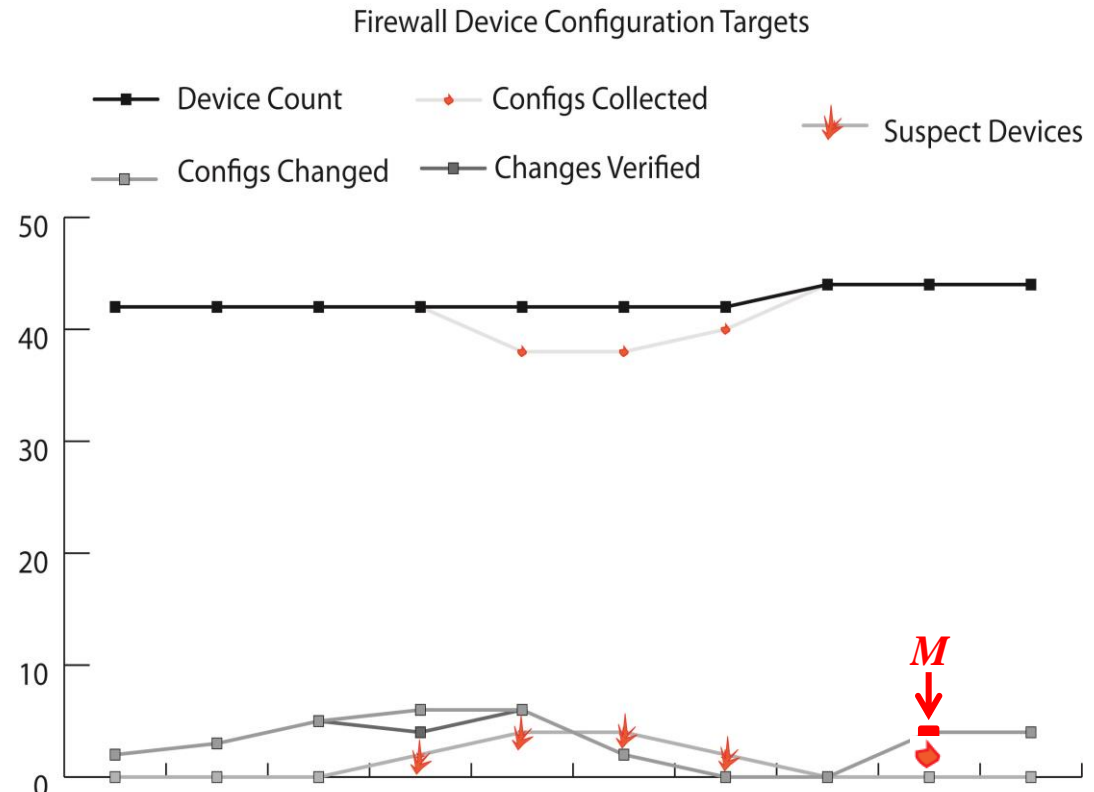
The number of firewall devices whose configuration was retrieved in past 24 hours by network management system.

Daily Measure Y:

The number of firewall devices configurations that deviate from yesterday's configuration.

Daily Measure Z:

The number of deviant device configurations where deviations directly compare to authorized planned changes.



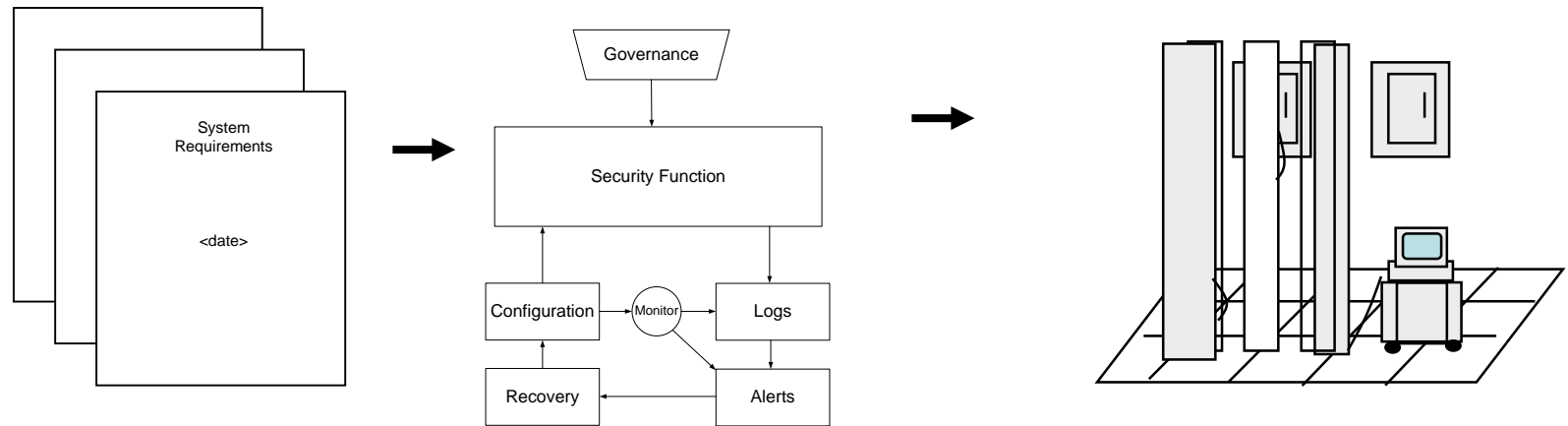
**Measure M:** The number of verified firewall changes that violate network security policy.

Daily Firewall Suspect Device Metric:  $((W-X) + (Y-Z)) / W$

Adjusted Metric for % Expected Error rate gleaned from monitoring :  $((W-X) + ((Y-Z) * 1.\%M)) / W$



# Requirements → Model Architecture → Technical Specifications



Vulnerabilities	!=	Exploits
Threats	!=	Exploits
Vulnerabilities + Threats	!=	Exploits
Vulnerabilities + Threats	allow	Exploits
Vulnerabilities + Threats + Prevention Process	minimize	Exploits

Exploits	!	Damage
Exploits + Service/Data/Financial Loss	=	Damage
Exploits + Service/Data /Financial Loss + Detection and Recovery Process	minimize	Damage