May 30, 2018 Conference

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

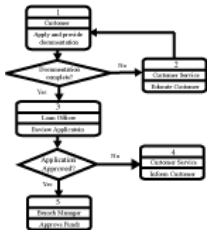
manage

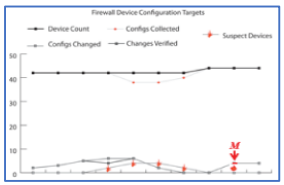
Cybersecurity Risk!

State of the Practice

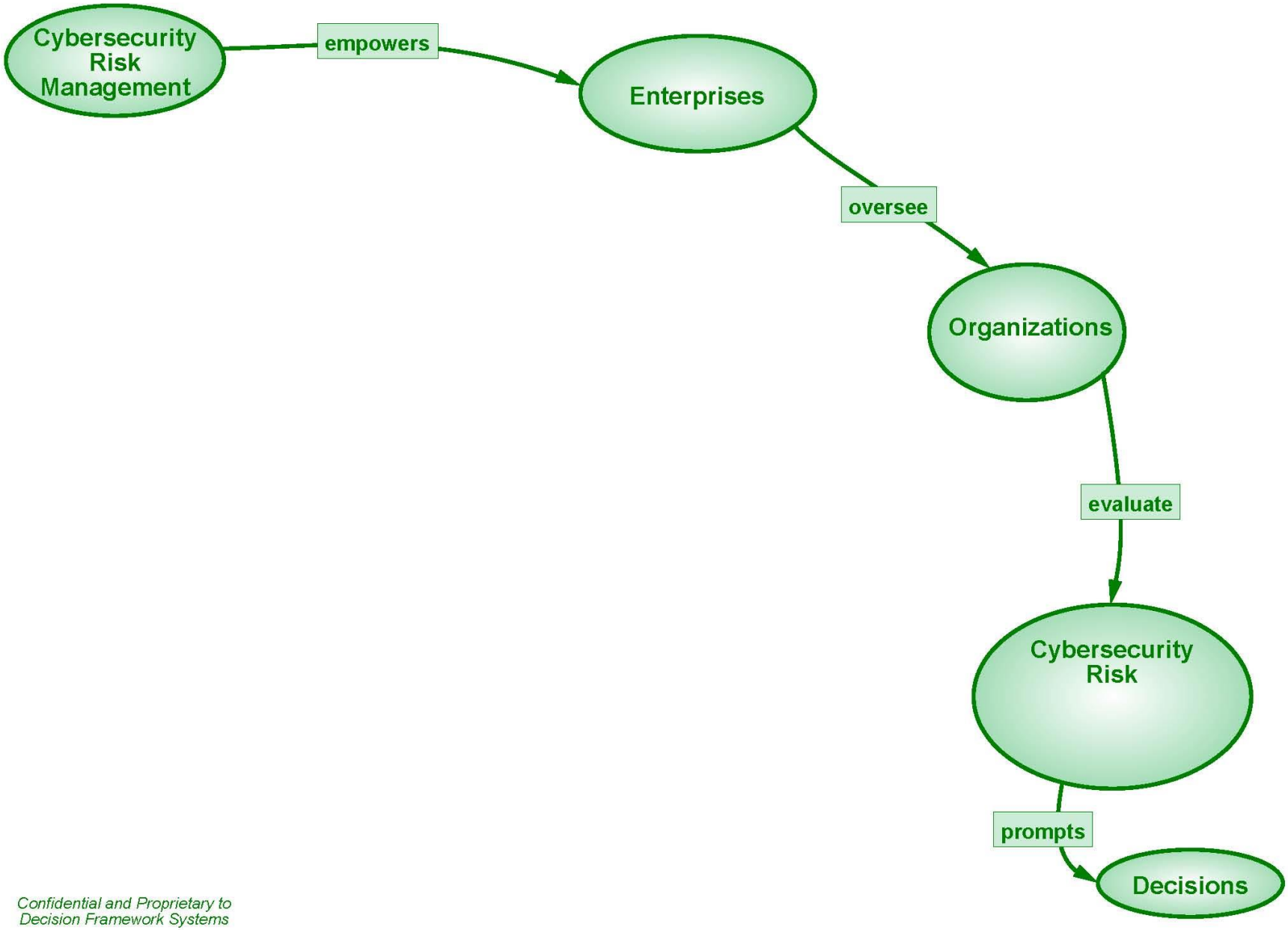
Existing Approach:	Cybersecurity Risk Assessment tools are prolific. They focus on well-defined subsets of the cybersecurity landscape and encompass a wide variety of disparate evaluation criteria, such as control gaps, maturity levels, and tiers.
Problem Statement:	Most individual cybersecurity assessors, 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.

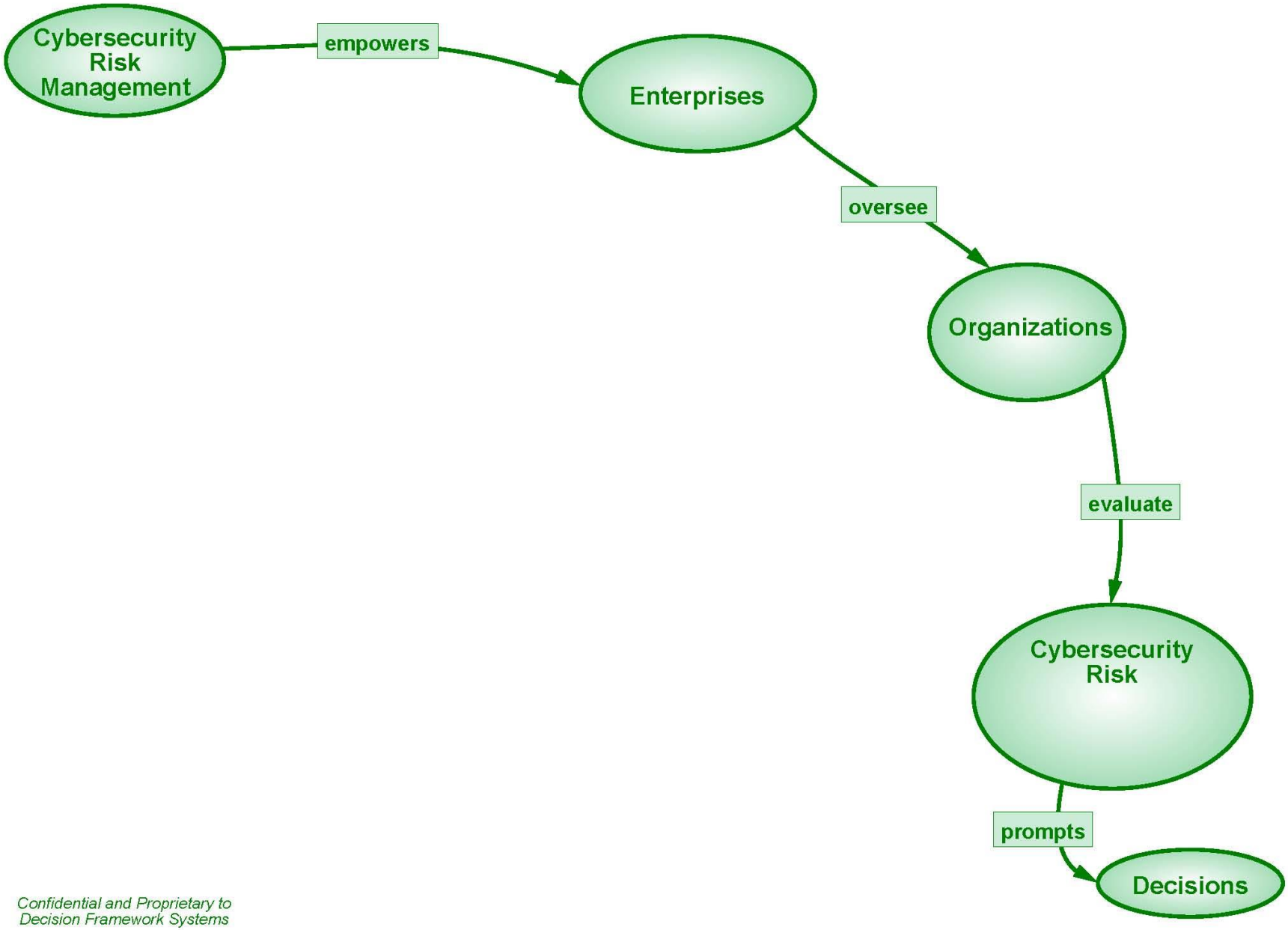
Framework Definitions

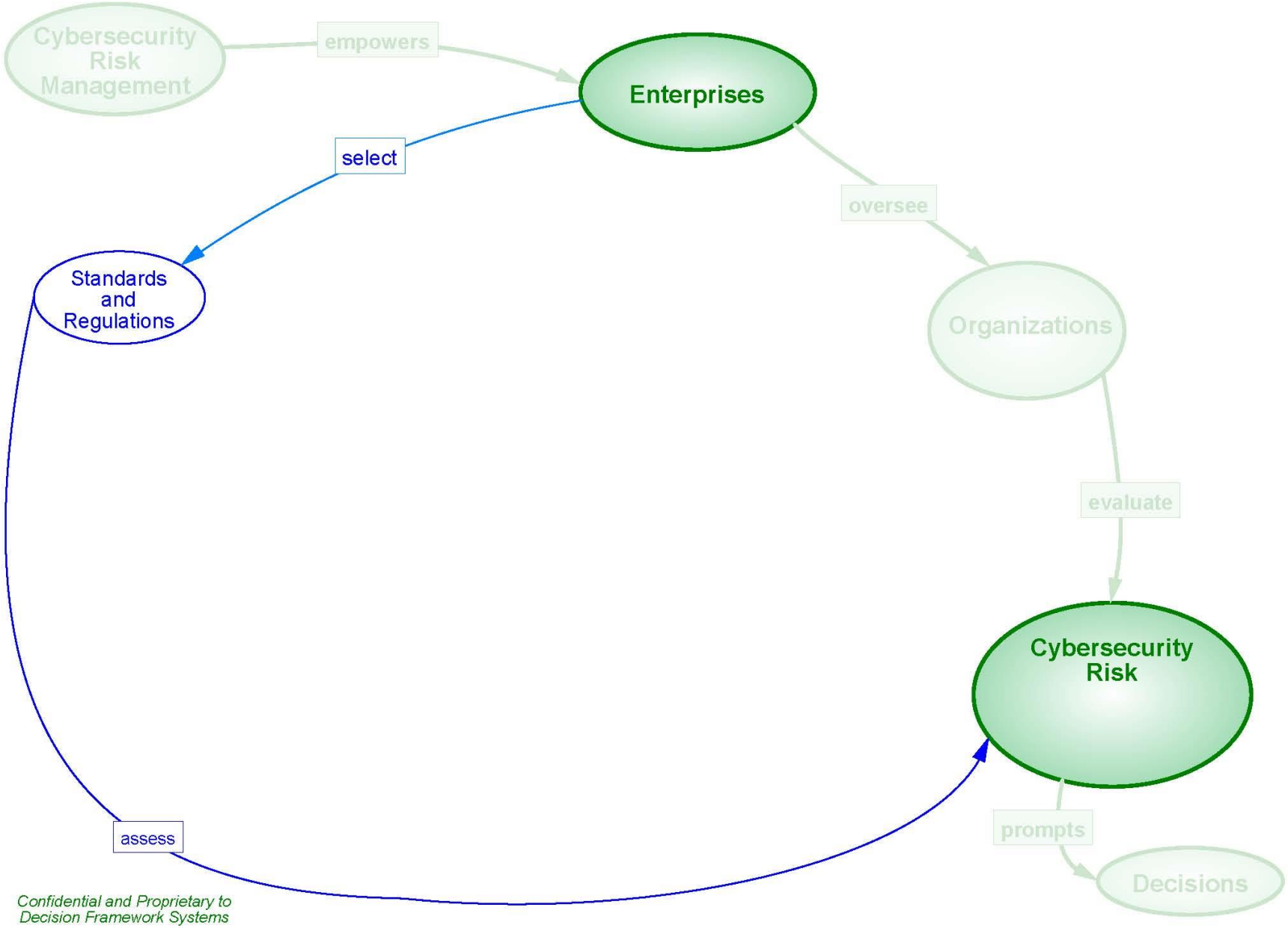


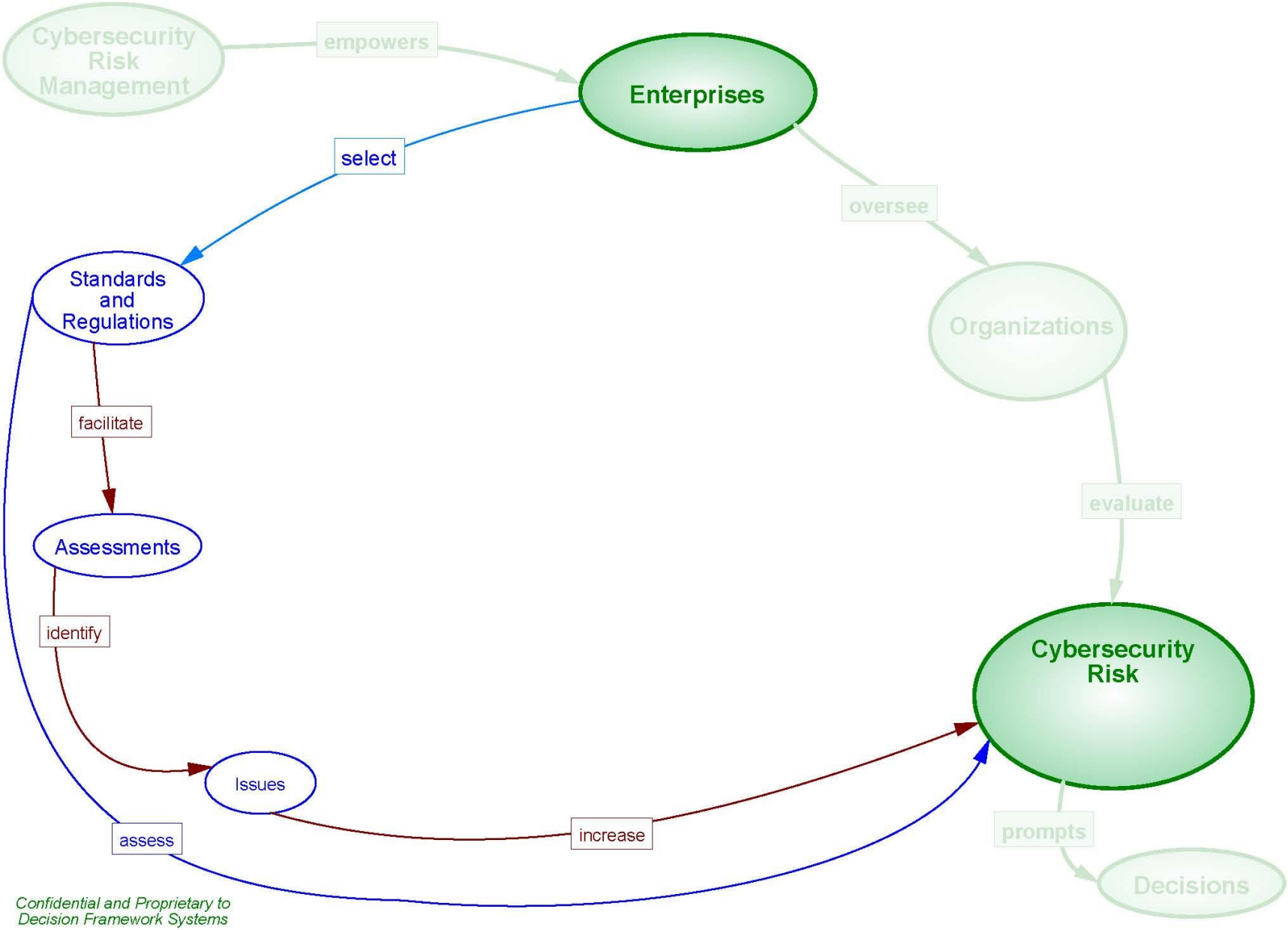


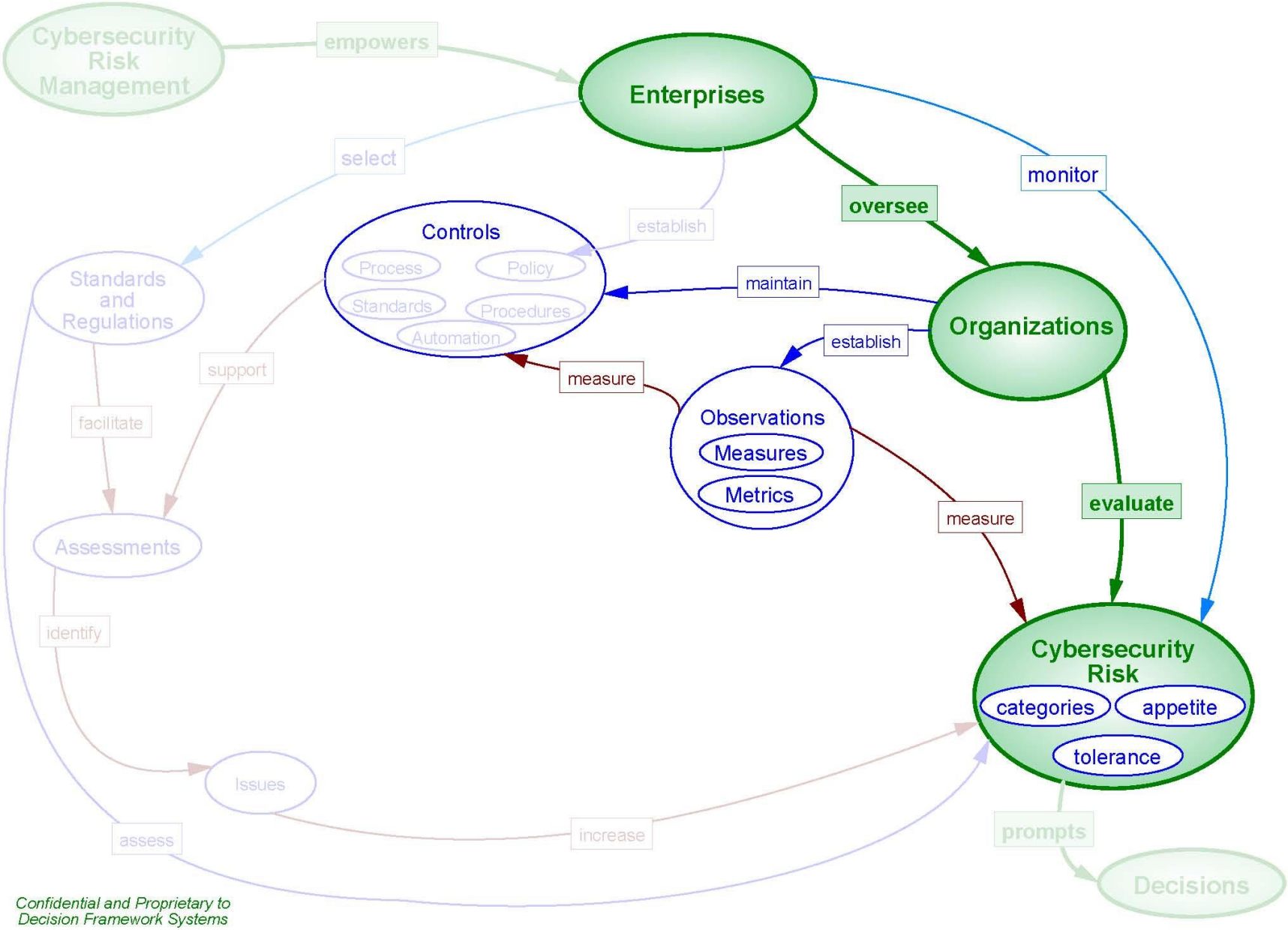
- ***Events*** are incidents of interest to risk management. They may happen within the organization, or to an external organization whose experience may have consequences for the organization, including potential increase in probability of similar events happening internally. Events may also be hypothetical exercises in risk awareness, and these are called Scenarios.
- ***Assessments*** are sets of requirements supplied by a guide plus several response fields that allow an assessor to document evidence that the requirements are or are not met. They are typically not used for risk reporting, but for Compliance.
- ***Issues*** are indications of vulnerability to risk. They are typically control weaknesses, but may be any circumstance that may indicate potential for an increase in risk. They are typically identified via assessments and events, but may also be self-identified.
- ***Controls*** are risk reduction measures. They may be directly enumerated, or may be documented as policies, processes, standards, procedures, or automation.
- ***Measures*** are maps from the empirical world to the formal, relational world, taken to characterize some object under scrutiny. Cybersecurity is not an empirical object, and not subject to direct measure.
- ***Cybersecurity Metrics*** are combinations of measures that, taken together, can provide information about cybersecurity.
- ***Risks*** are categories of events that present potential negative impact to the Enterprise. Risks are associated with a qualitative risk appetite and quantitative tolerance measures.

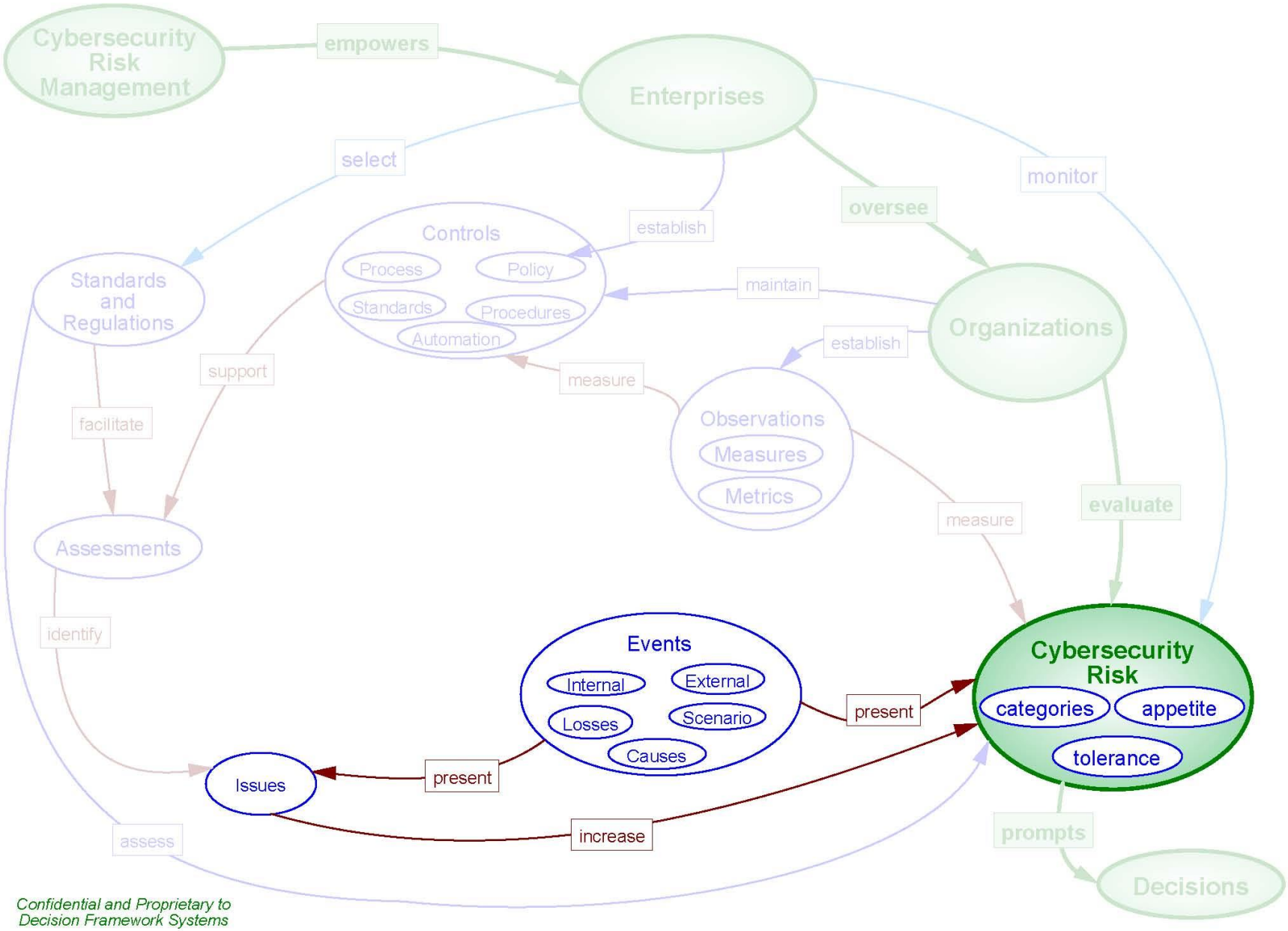


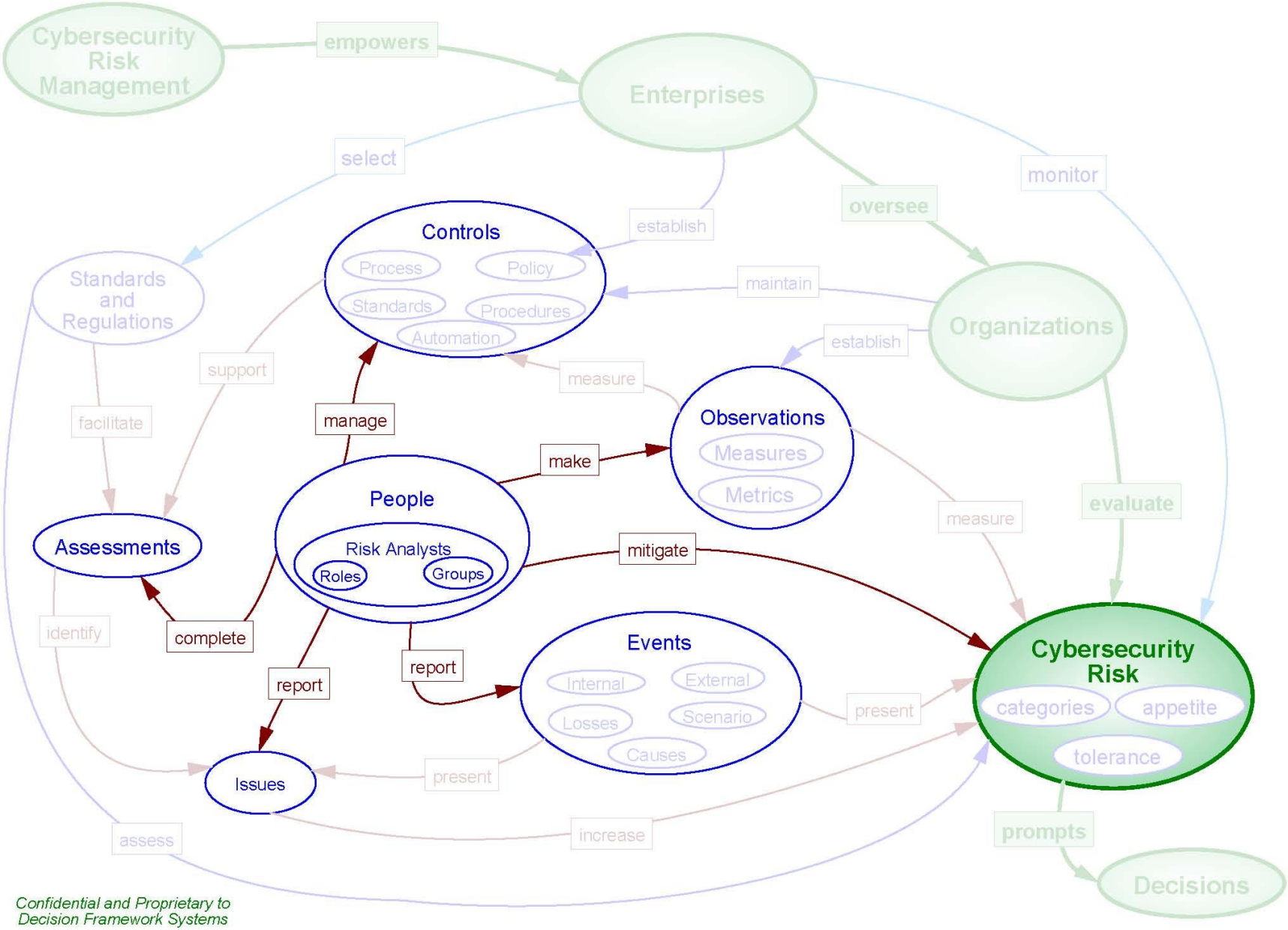


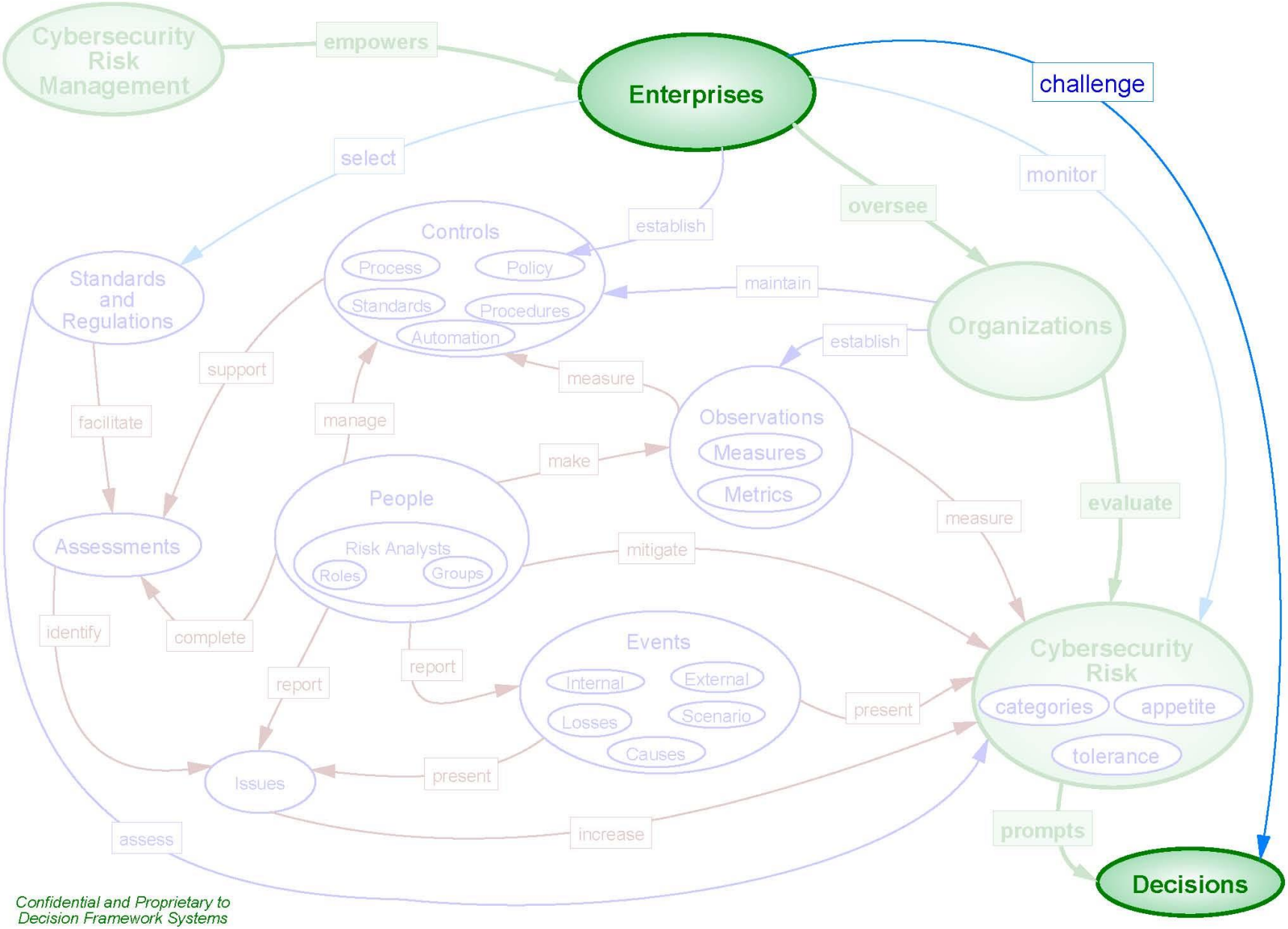


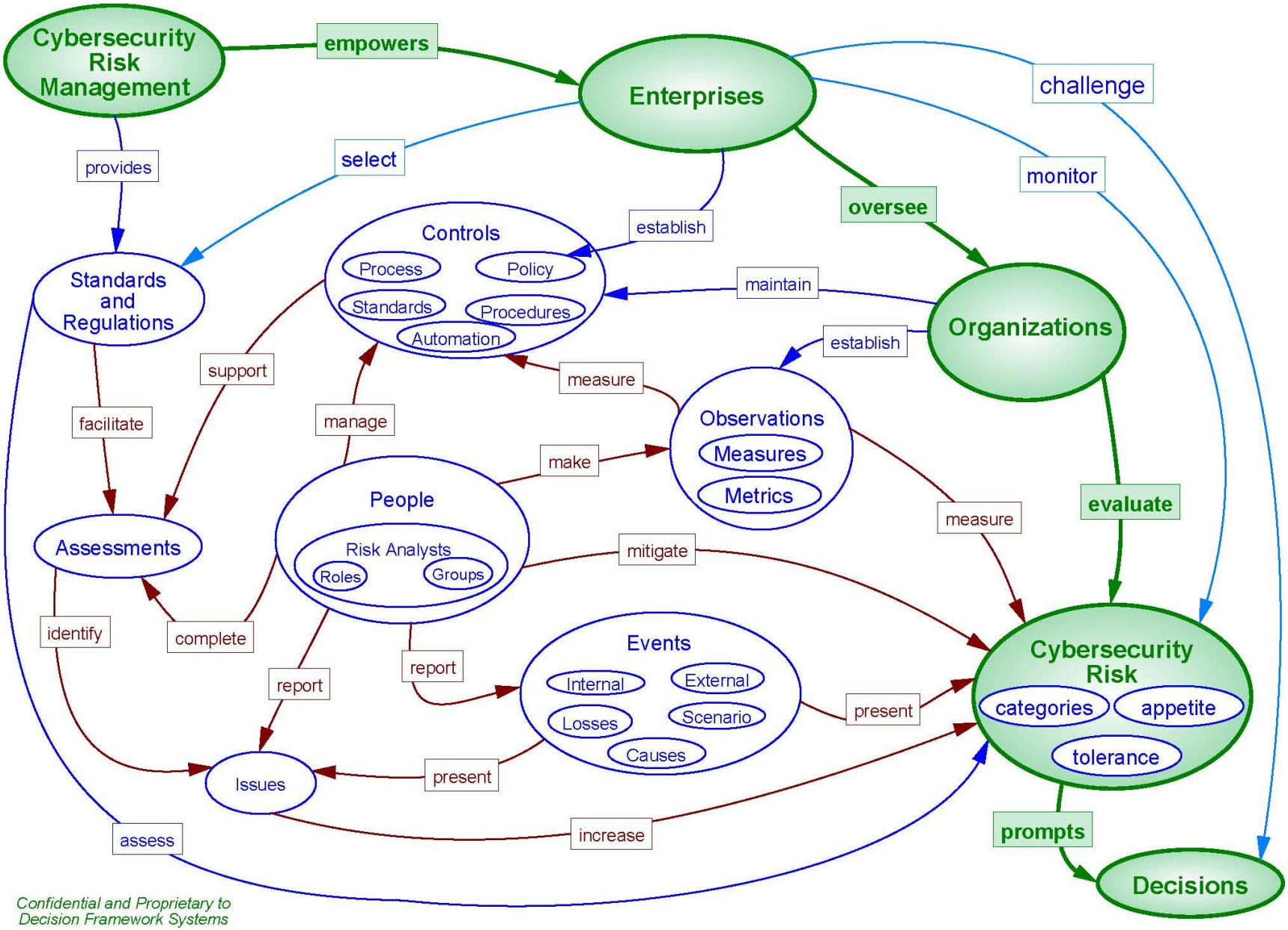




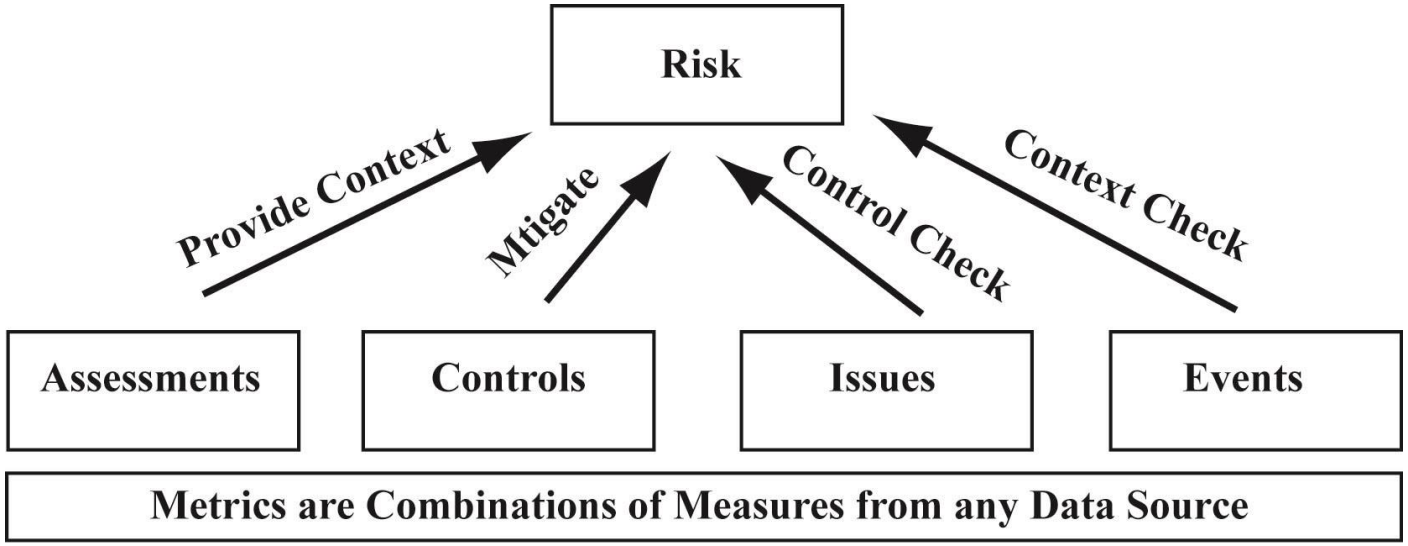






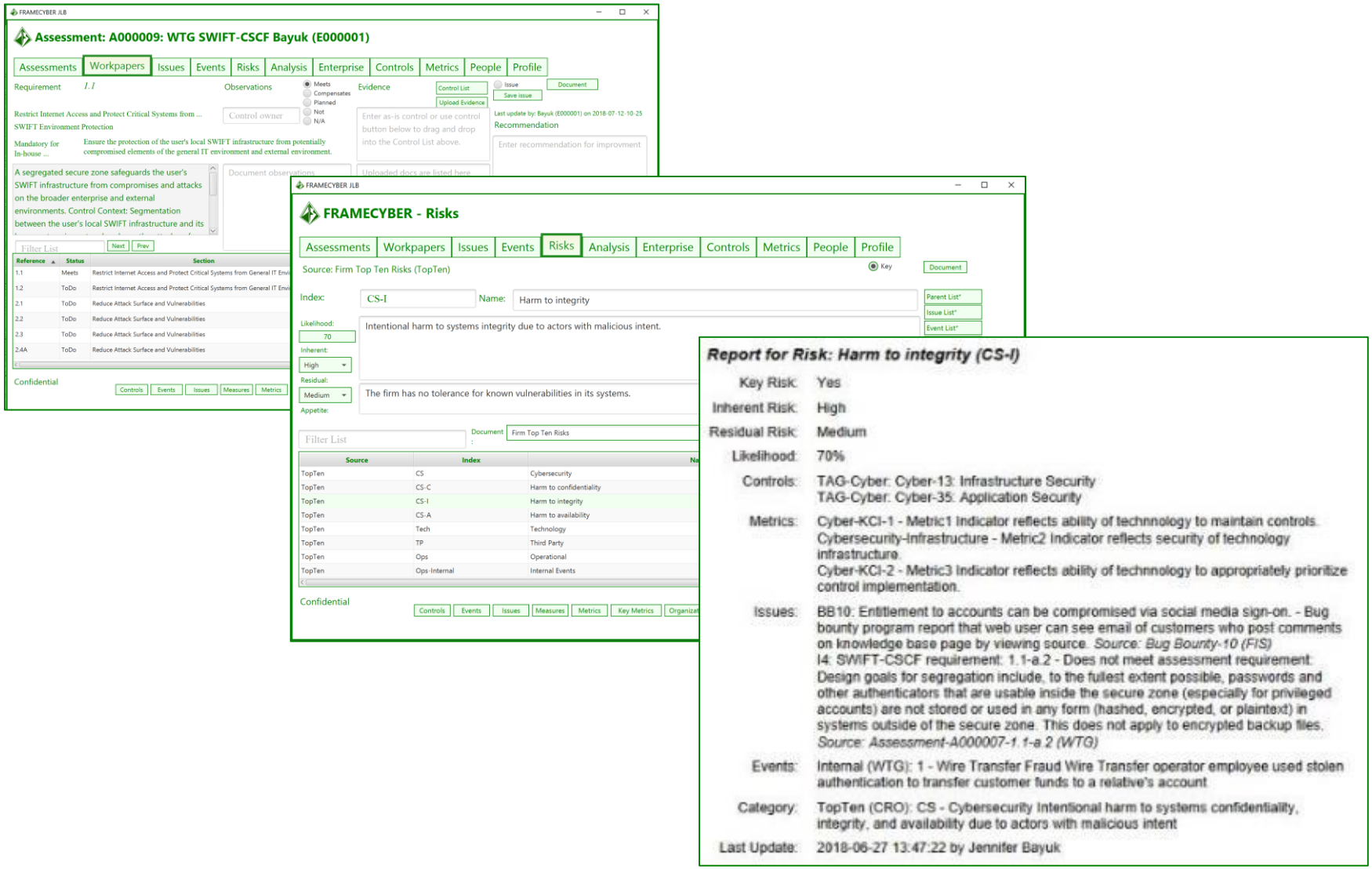


Quantitative Data Analysis



- 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



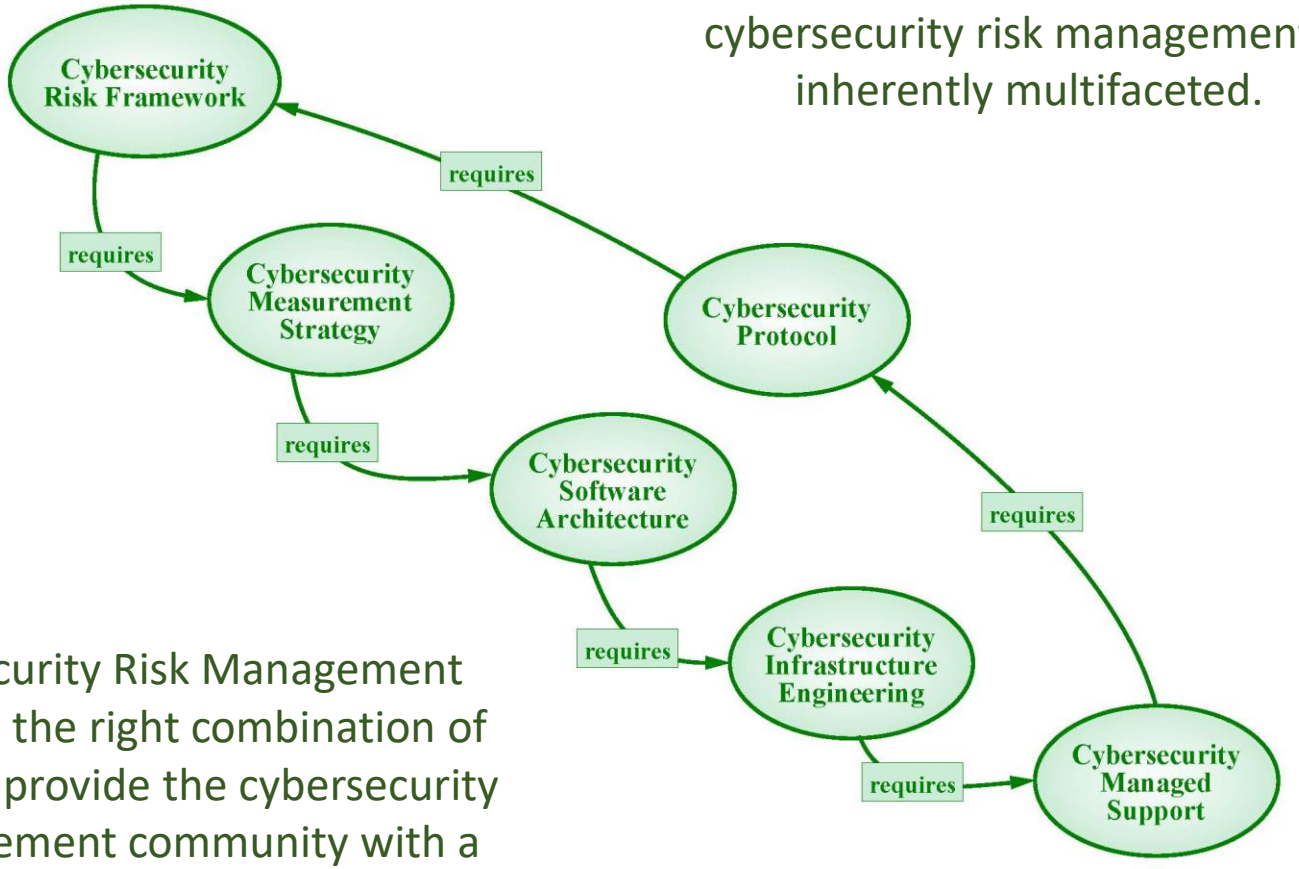
See http://www.framecyber.com

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.

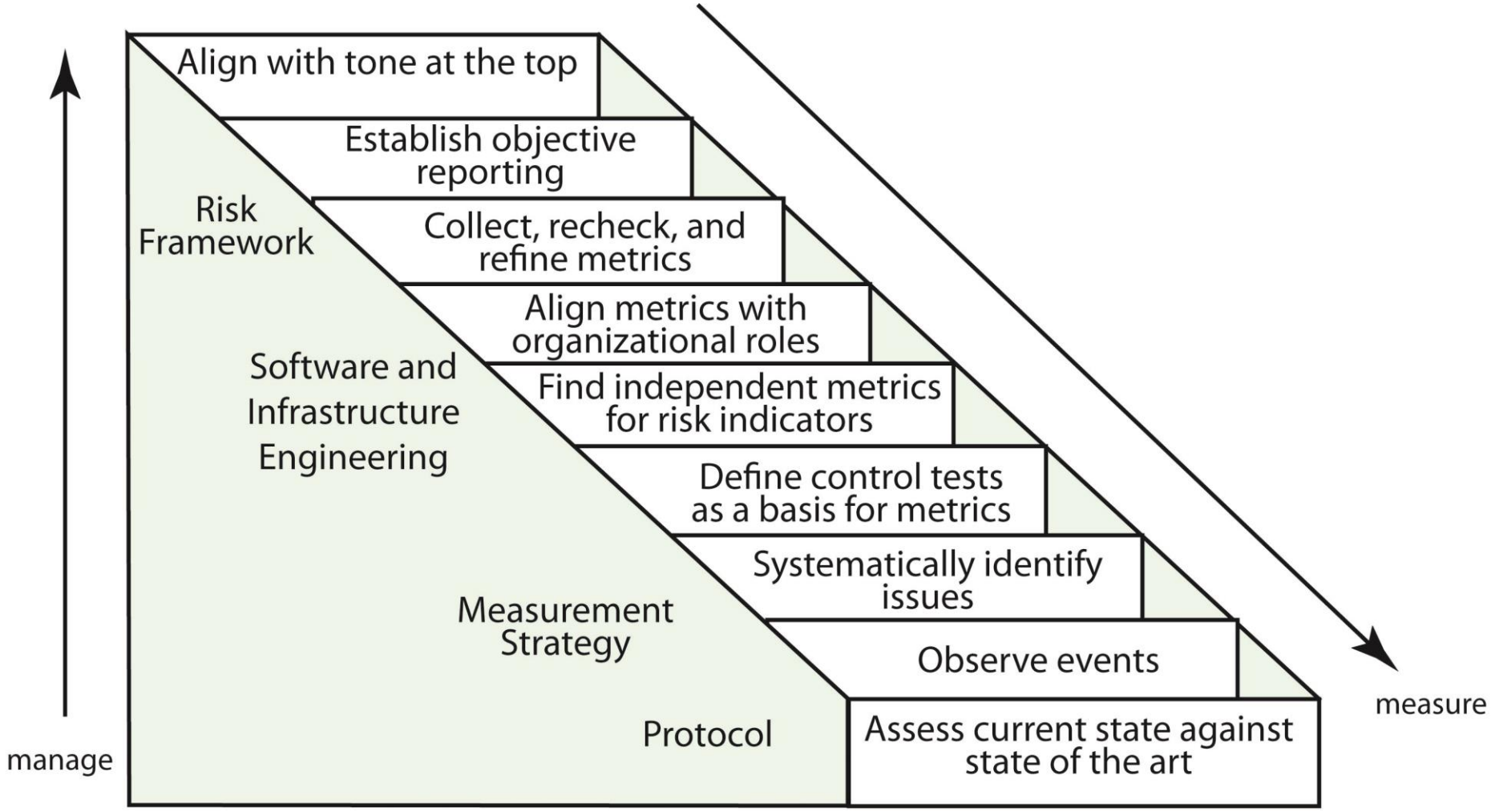
Cybersecurity Risk Team Roles and Responsibilities

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

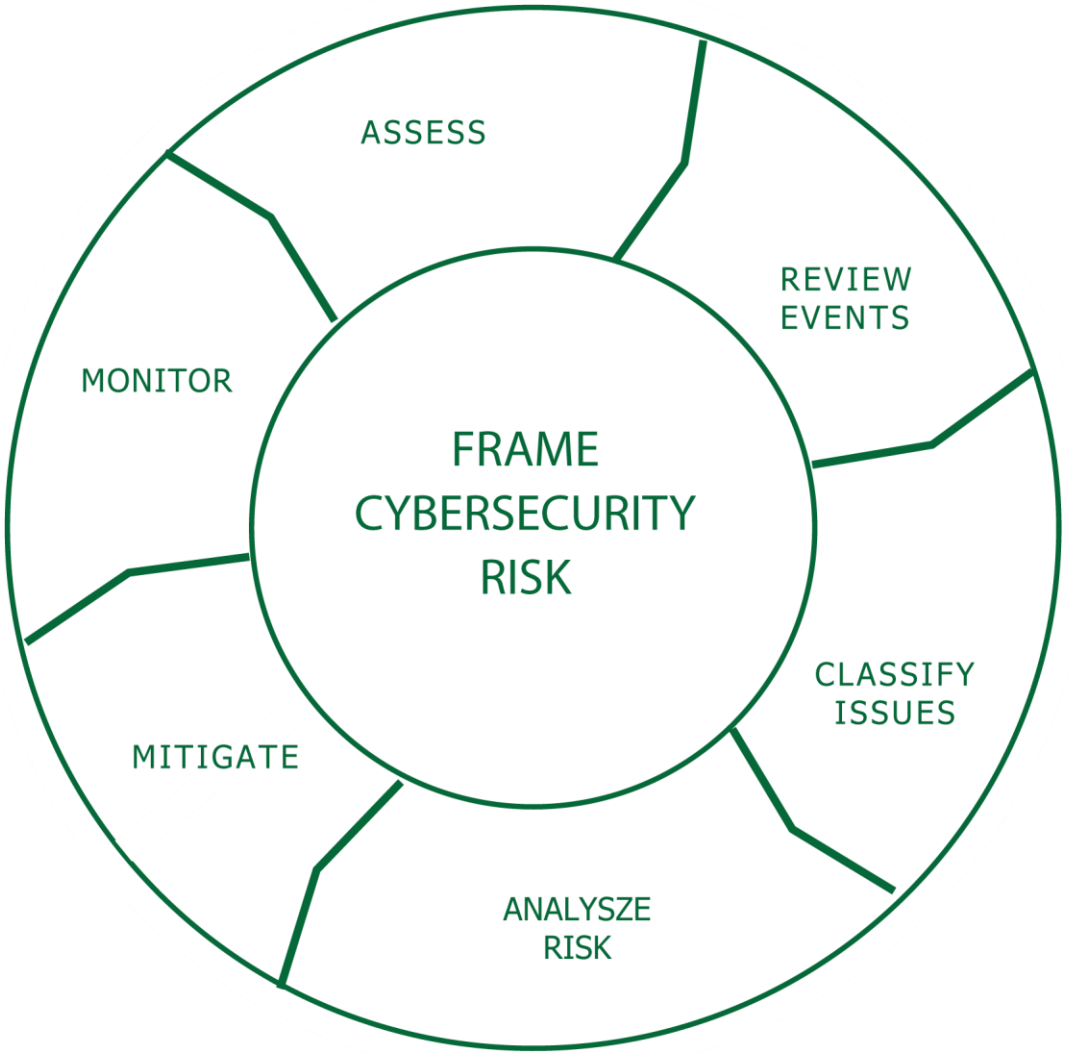


A Cybersecurity Risk Management team needs the right combination of expertise to provide the cybersecurity risk management community with a reliable, repeatable, and maintainable continuous cybersecurity risk assessment framework

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
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.	**ID.GV-4**: Governance and risk management processes address cybersecurity risks. (p. 22) **ID.RM-1:** 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	**ID.GV-4:** 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:

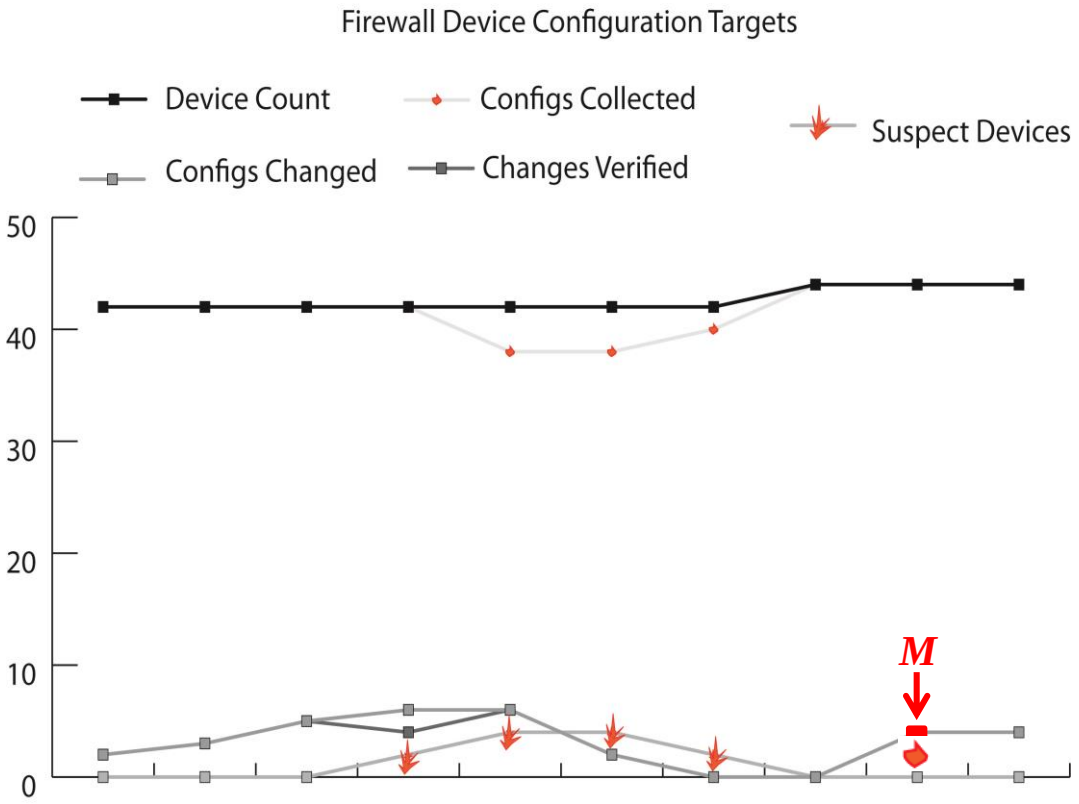
The number of firewall devices whose configuration was retrieved in past 24 hours by network management system.

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.

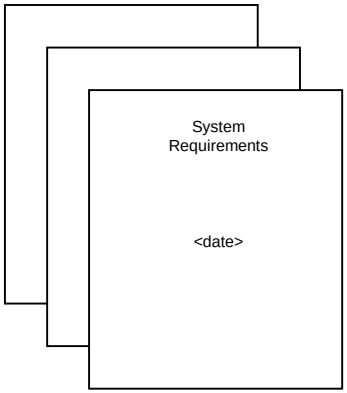


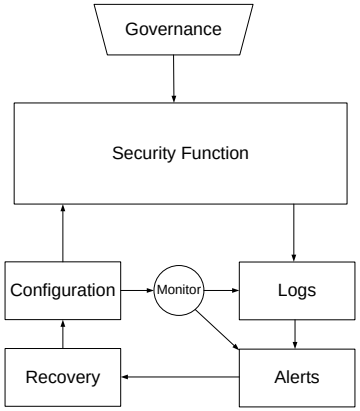
Measure M: The number of verified firewall changes that violate network security policy.

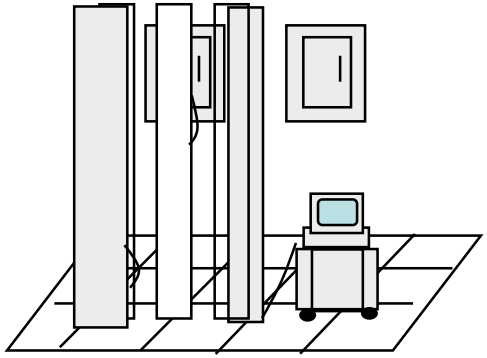
Daily Firewall Suspect Device Metric: ((W-X) + (Y-Z)) / W

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