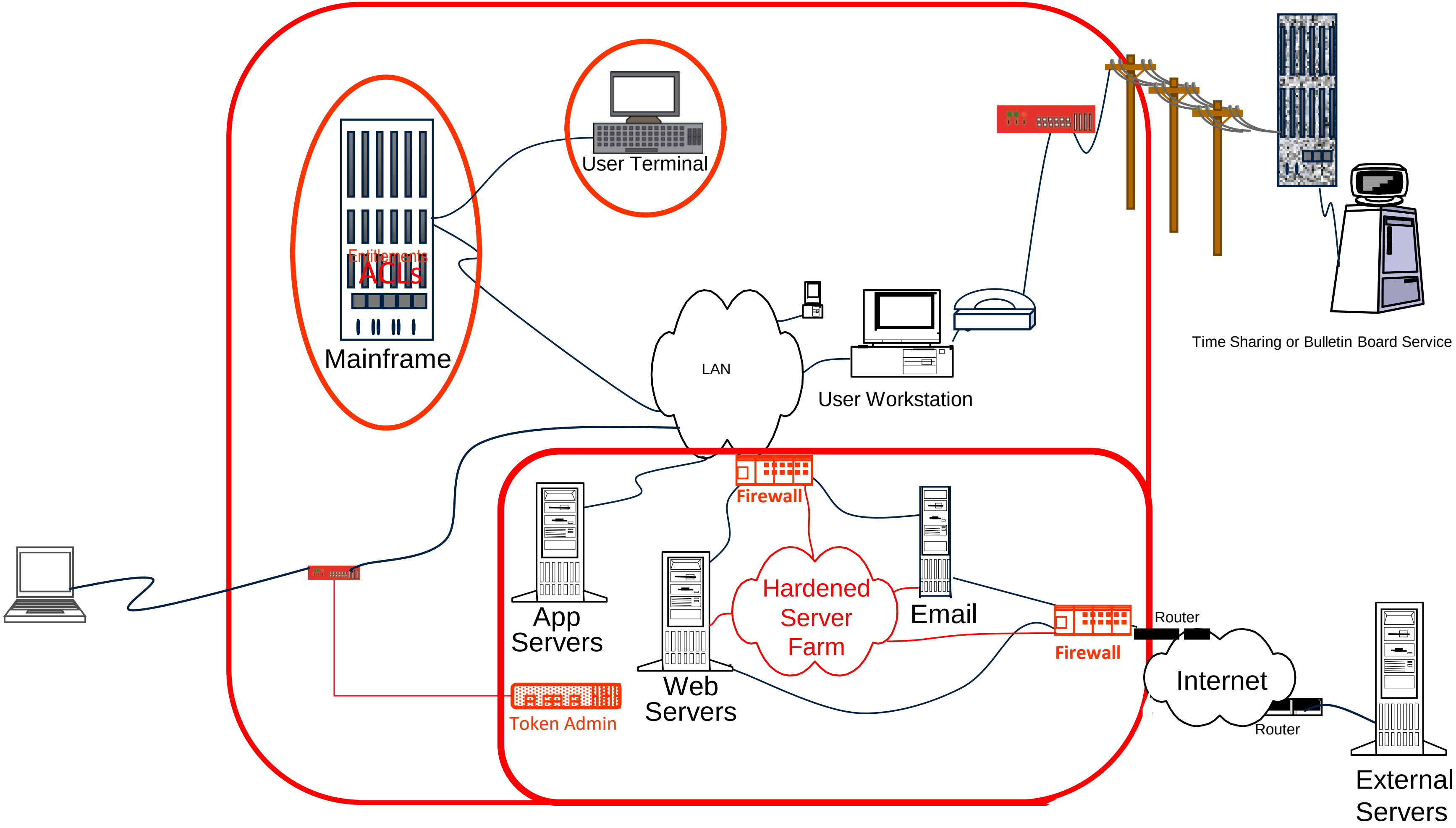
A Framework for Cybersecurity Risk

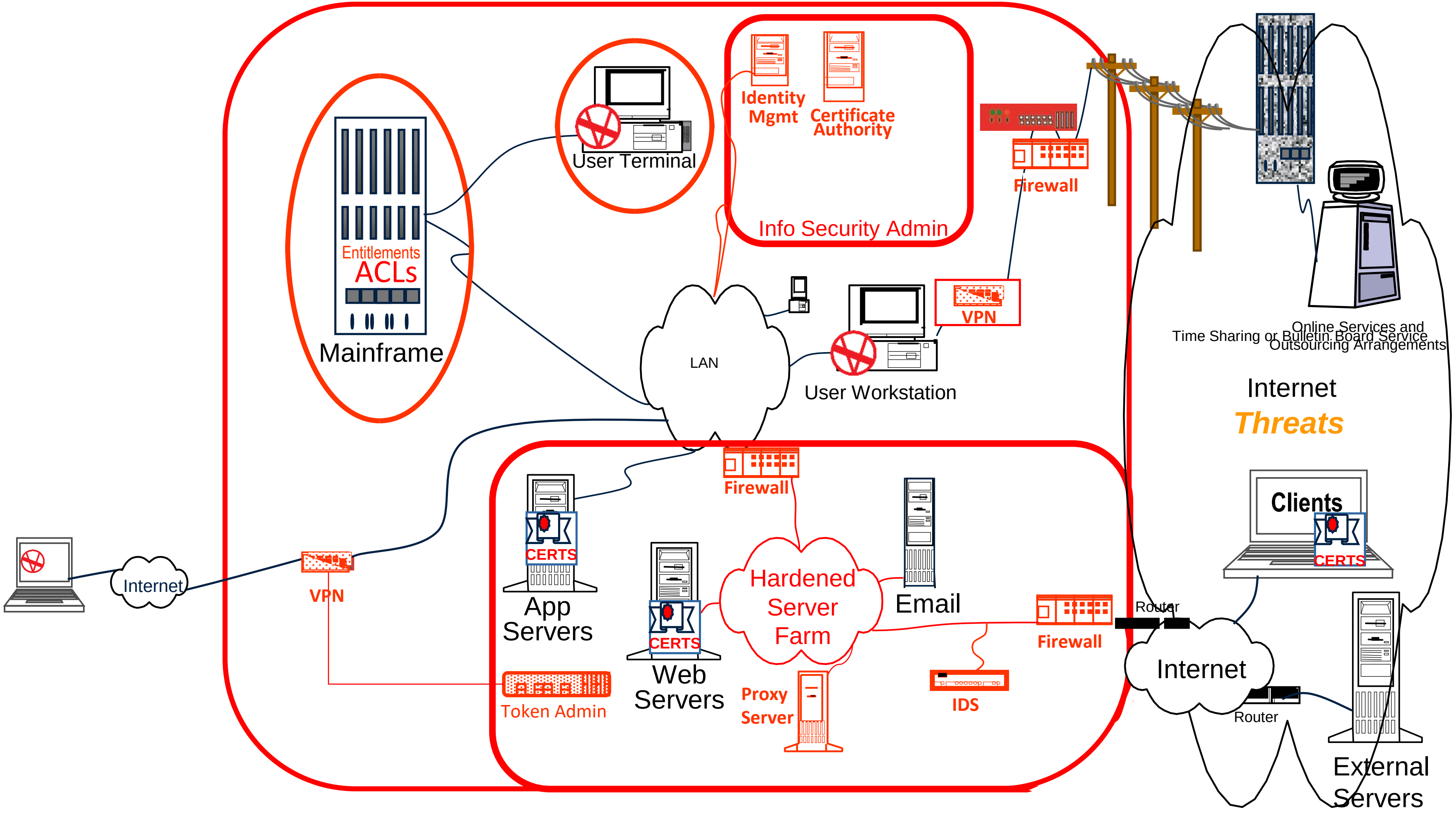
SIRACON 2019

Jennifer Bayuk

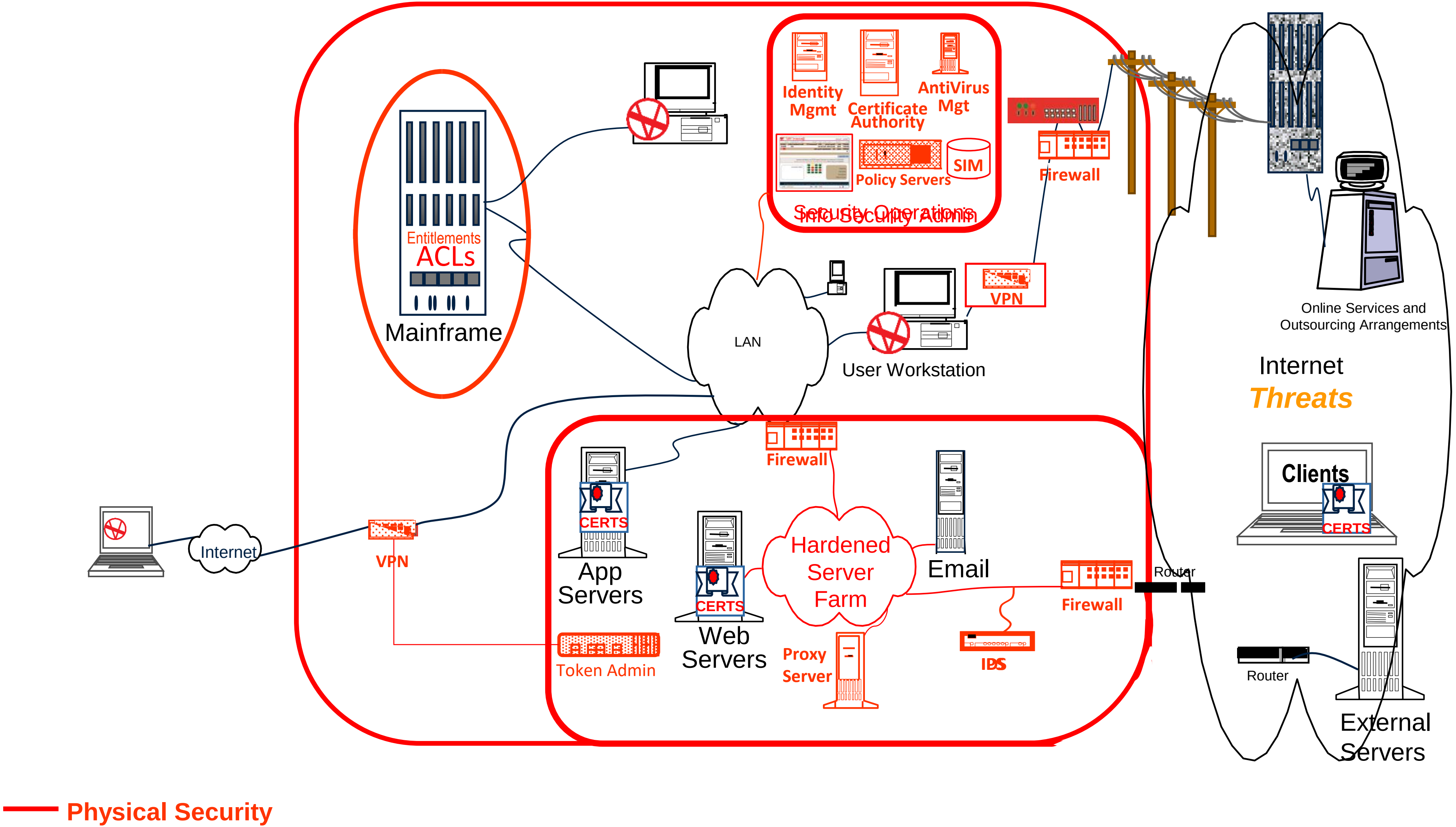
Decision Framework Systems, Inc.

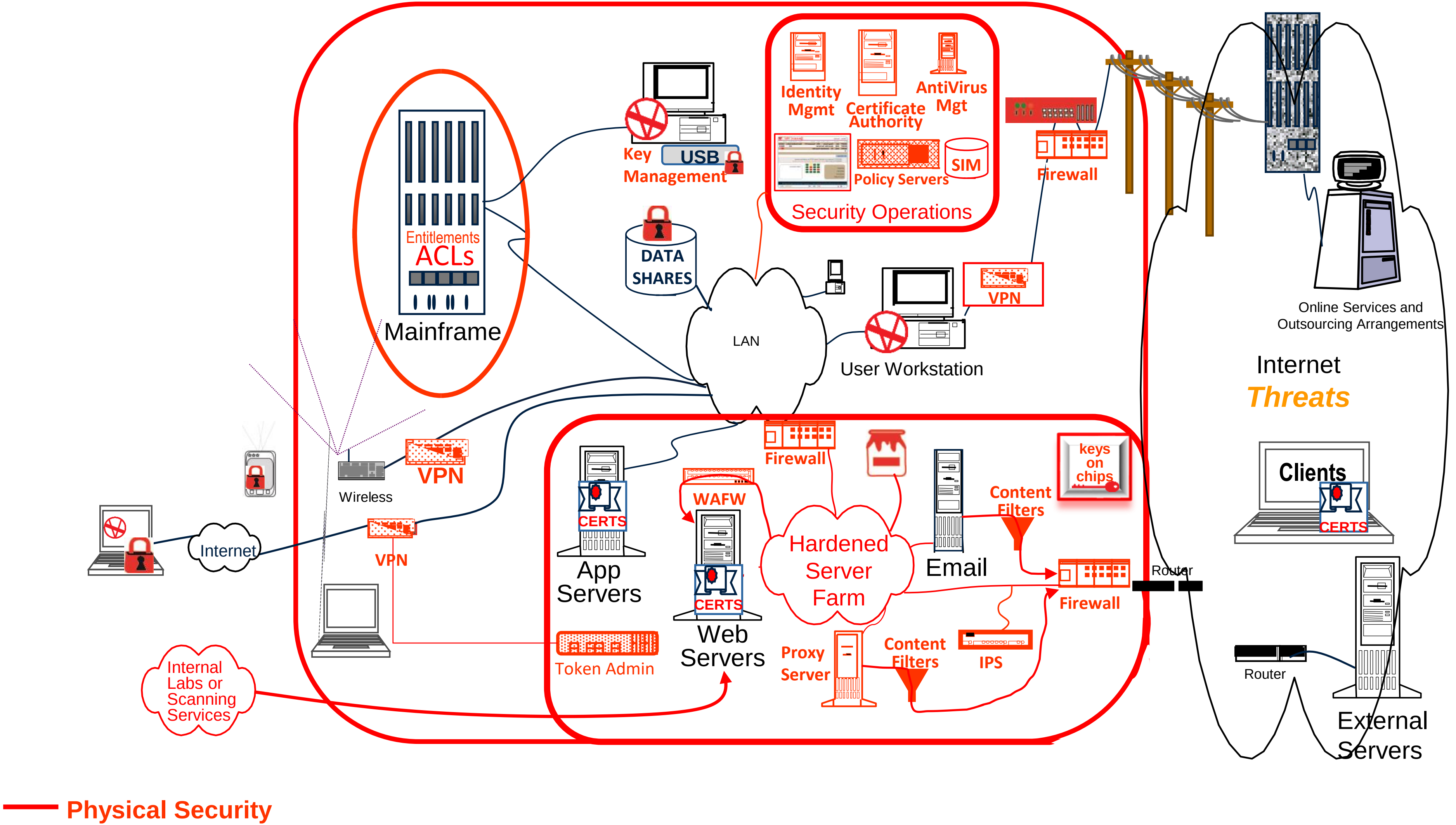


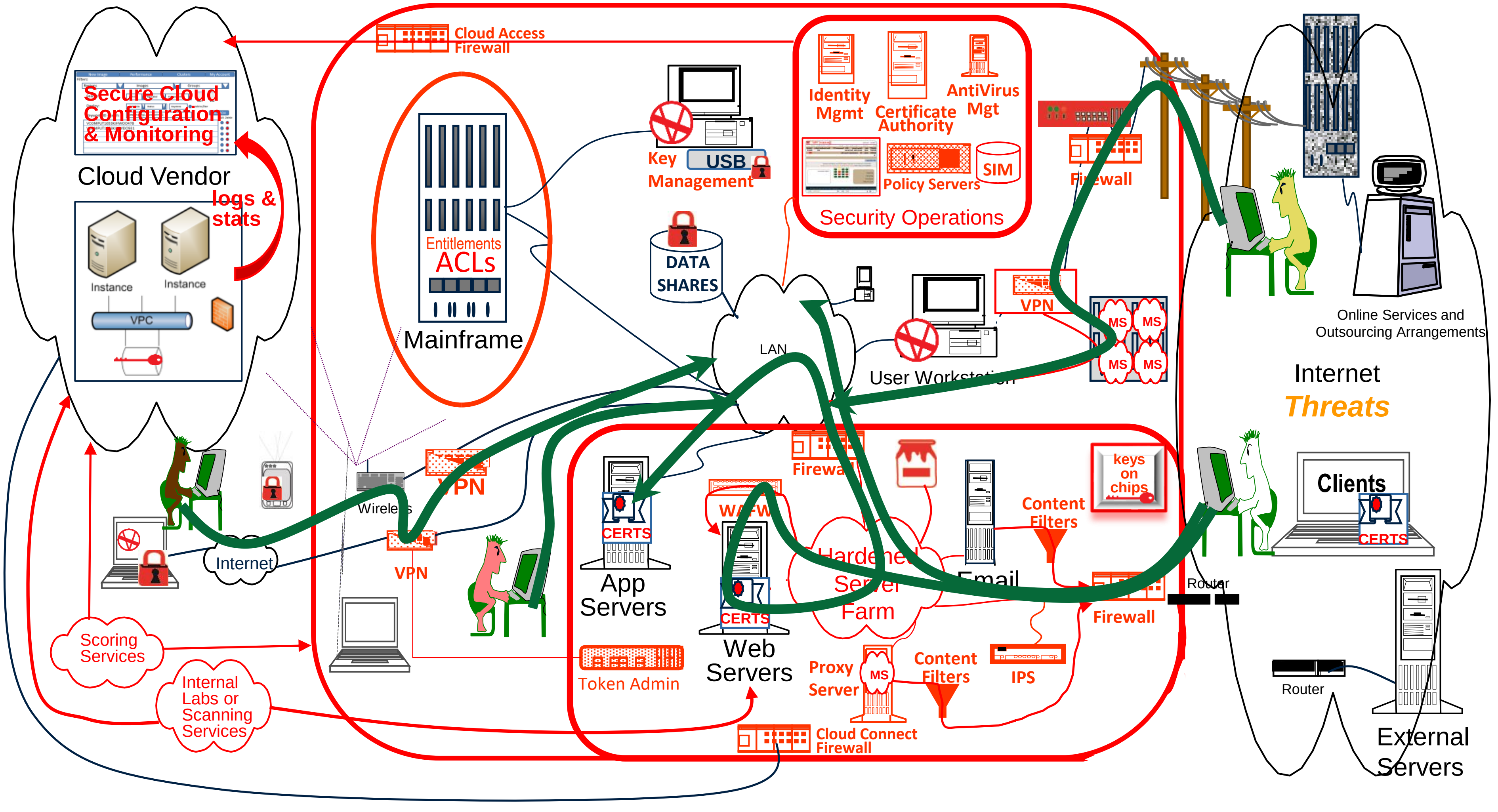
— Physical Perimeter



— **Physical Security**

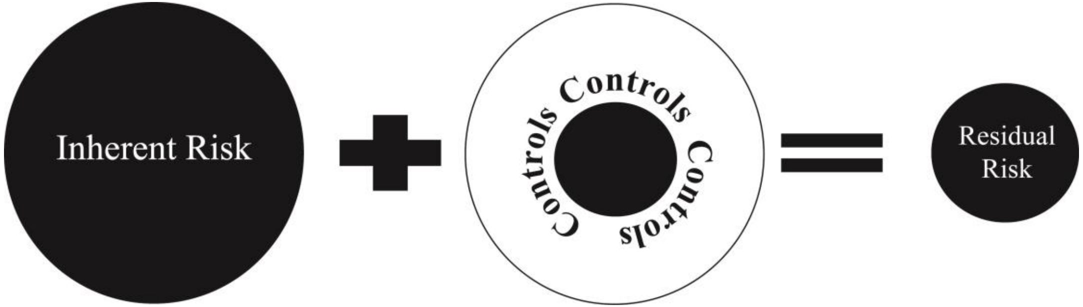

Identity
Mgmt
Certificate
Authority
AntiVirus
Mgt
Policy Servers
SIM
Security Operations
Info Security Admin
Firewall
Entitlements
ACLs
Mainframe
LAN
VPN
User Workstation
Online Services and
Outsourcing Arrangements
Internet
Threats
Clients
CERTS
Internet
VPN
CERTS
App
Servers
CERTS
Web
Servers
Firewall
Hardened
Server
Farm
Email
Firewall
Router
IDS
Proxy
Server
Token Admin
Router
External
Servers
Physical Security


Entitlements
ACLs
Mainframe
Key
USB
Management
DATA
SHARES
Identity
Mgmt
Certificate
Authority
AntiVirus
Mgt
Policy Servers
SIM
Security Operations
Firewall
LAN
VPN
User Workstation
Online Services and
Outsourcing Arrangements
Internet
Threats
Wireless
VPN
Internet
VPN
Firewall
WAFW
CERTS
App
Servers
CERTS
Web
Servers
Hardened
Server
Farm
Email
keys
on
chips
Content
Filters
Firewall
Router
Clients
CERTS
Token Admin
Proxy
Server
Content
Filters
IPS
Router
External
Servers
Internal
Labs or
Scanning
Services
Physical Security

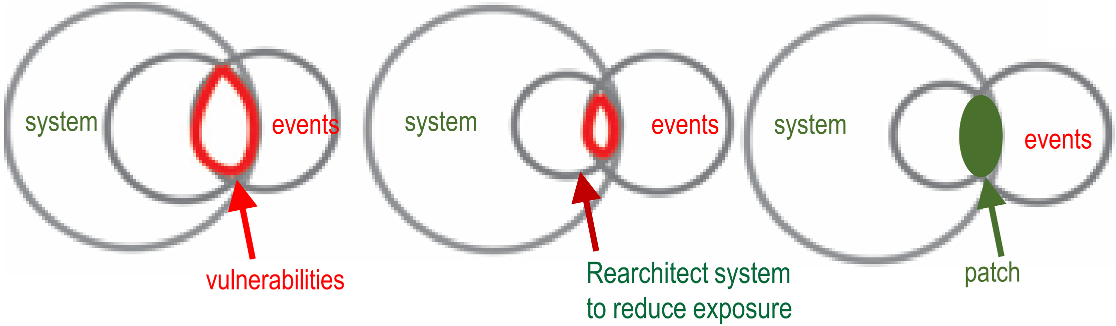


▬ **Physical Security**

Operational Risk Measurement 101

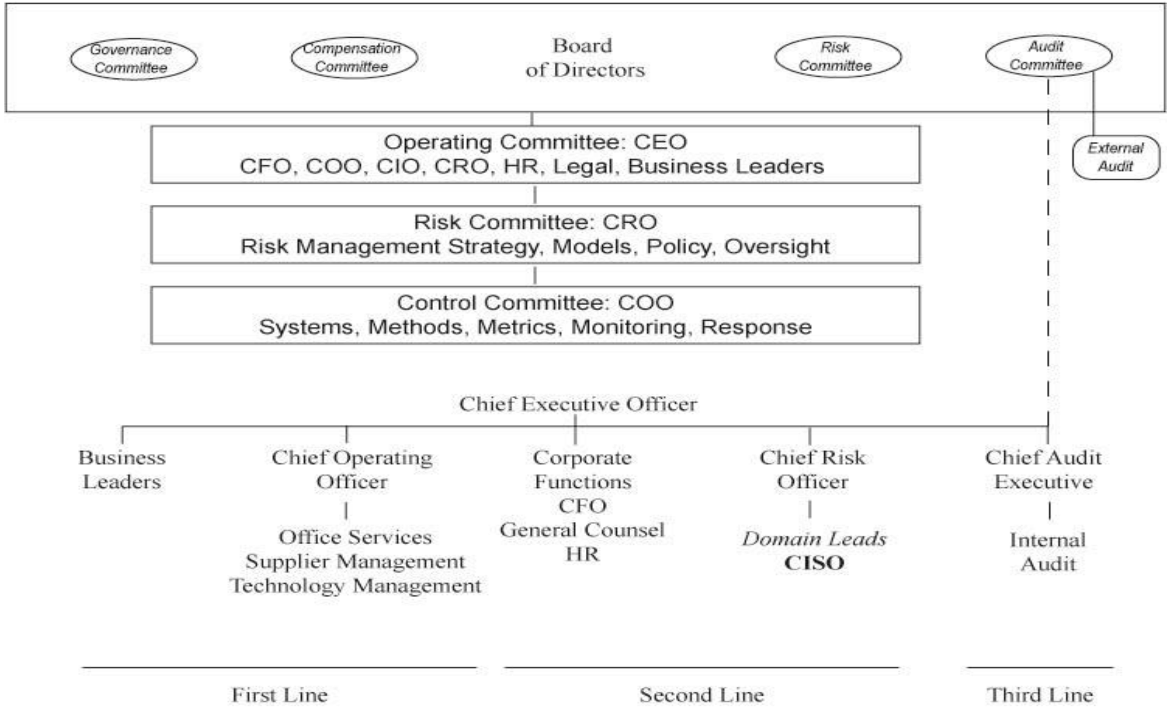


Technology-Specific Version
measure exposure to negatively-impacting events



Why a Cybersecurity Risk Management Framework?

A shared understanding of *management strategy for keeping risk to an acceptable level*, or *Risk Management Framework* is essential for any independent party to properly interpret management activities and metrics.



Why not just Adopt the NIST Cybersecurity Framework?

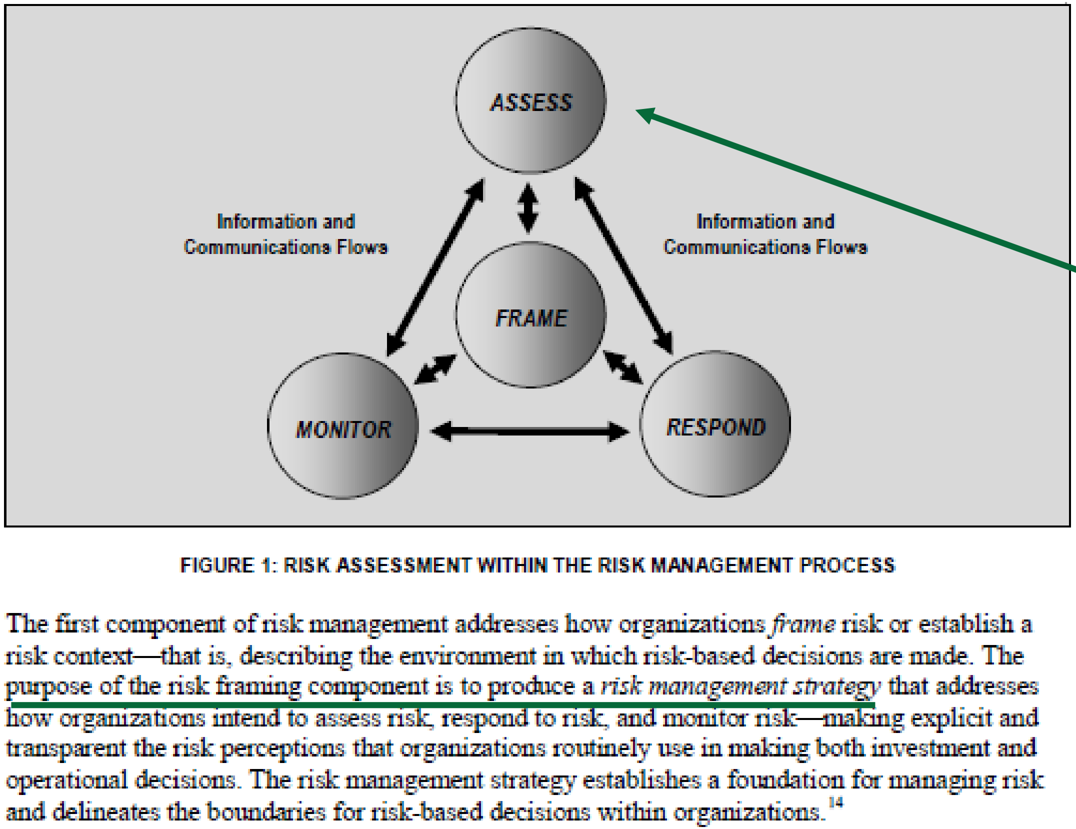

ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

FIGURE 1: RISK ASSESSMENT WITHIN THE RISK MANAGEMENT PROCESS

The first component of risk management addresses how organizations *frame* risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a *risk management strategy* that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk management strategy establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations.[14]

- *NIST SP800-30, Guide for Conducting Risk Assessments*

Because it is not what we mean by Framework.

Rather, it is an assessment tool, even by NIST’s definition.

- *See NIST CSF, Version 1.1 Section 4*

Why not just use BASEL* Operational Risk Framework?

BASEL Framework Elements:

- Internal Loss Data Collection and Analysis
- External Data Collection and Analysis
- Risk Assessments
- Business Process Mapping
- Risk and Performance Indicators
- Scenario Analysis
- Measurement
- Comparative Analysis

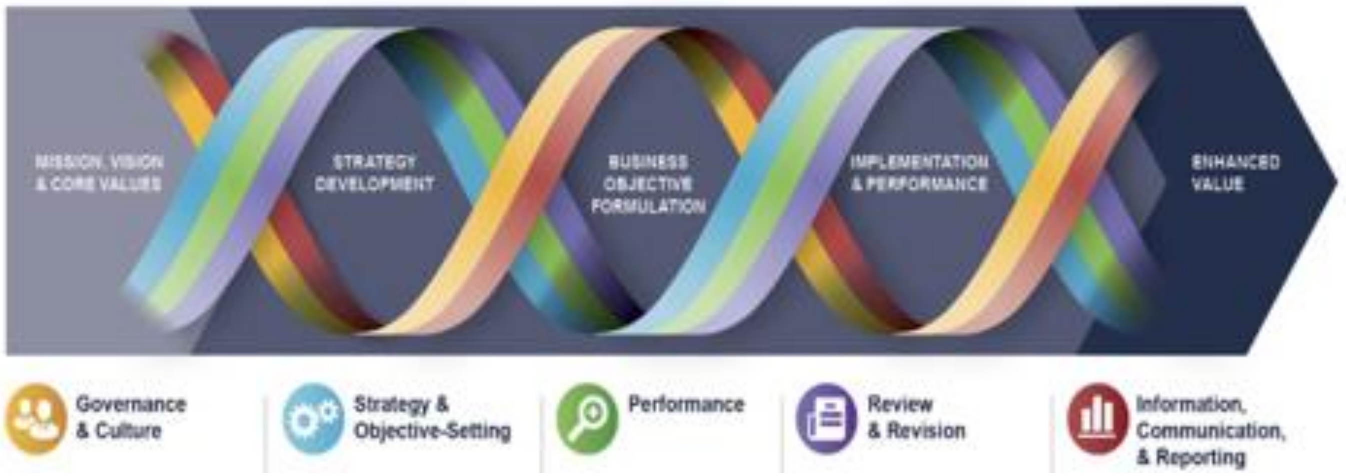
Because technology and cybersecurity risk is interspersed throughout BASEL risk categories, aggregate reporting requirements are difficult to meet without duplication. However, cybersecurity risk should be incorporated into BASEL event categories.

Overlap Between BASEL & Cybersecurity Risk Event Categories.

Internal Fraud	*Computer-Aided Fraud*
External Fraud	*Computer-Aided Fraud*
Employment Practices and Workplace Safety	
Clients, Products, and Business Practice	*Data Confidentiality and/or Integrity*
Damage to Physical Assets	
Business Disruption and Systems Failures	*Availability*
Execution, Delivery, and Process Management	

* Sound Practices for the Management and Supervision of Operational Risk (BCBS96) 2003, and subsequent enhancements to provide more detail on specific topics.

Why not just use COSO?



COSO is very broad, and does not provide guidance at the level of risk event type or category.

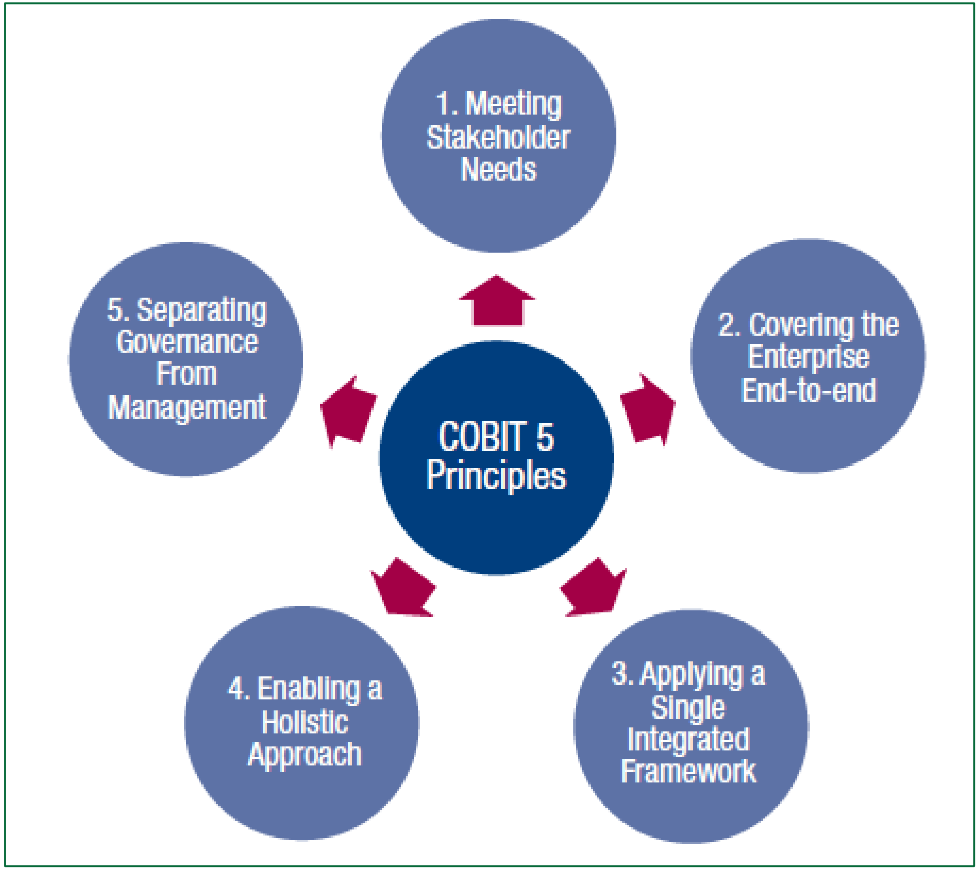
In COSO, a risk is ***any*** event that could impede *or promote* business objectives (market, credit, etc.).

* *COSO (2017). Enterprise Risk Management: Integrating with Strategy and Performance,* The American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), and the Institute of Management Accountants [IMA].

Why not just use COBIT[*]?

COBIT is a comprehensive set of best practices, but only part of the solution, it is a set of "Enablers" that support requirements that have to come from risk management.

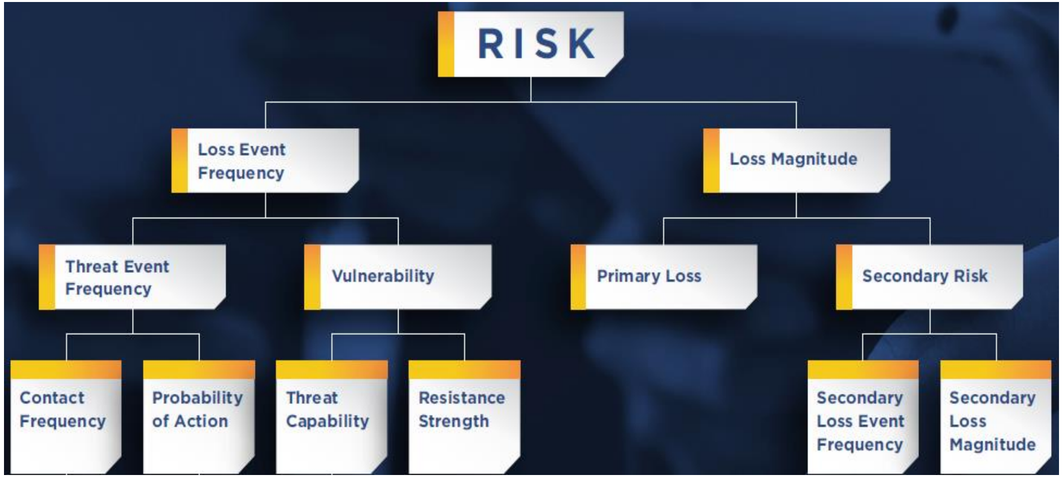
"When making necessary investments in technology or other infrastructure, management considers the tools required ***to enable*** *enterprise risk management activities." – COSO ERM*


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
COBIT 5 Principles
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management

[*] *Information Systems Audit and Control Association (ISACA), a membership-based association of technology risk and control professionals with ~400 local chapters worldwide. Its principal publication, formerly: "Control Objectives for Information Technology," now simply: COBIT, in version 5 added the subtitle: A Business Framework for the Governance and Management of Enterprise IT.*

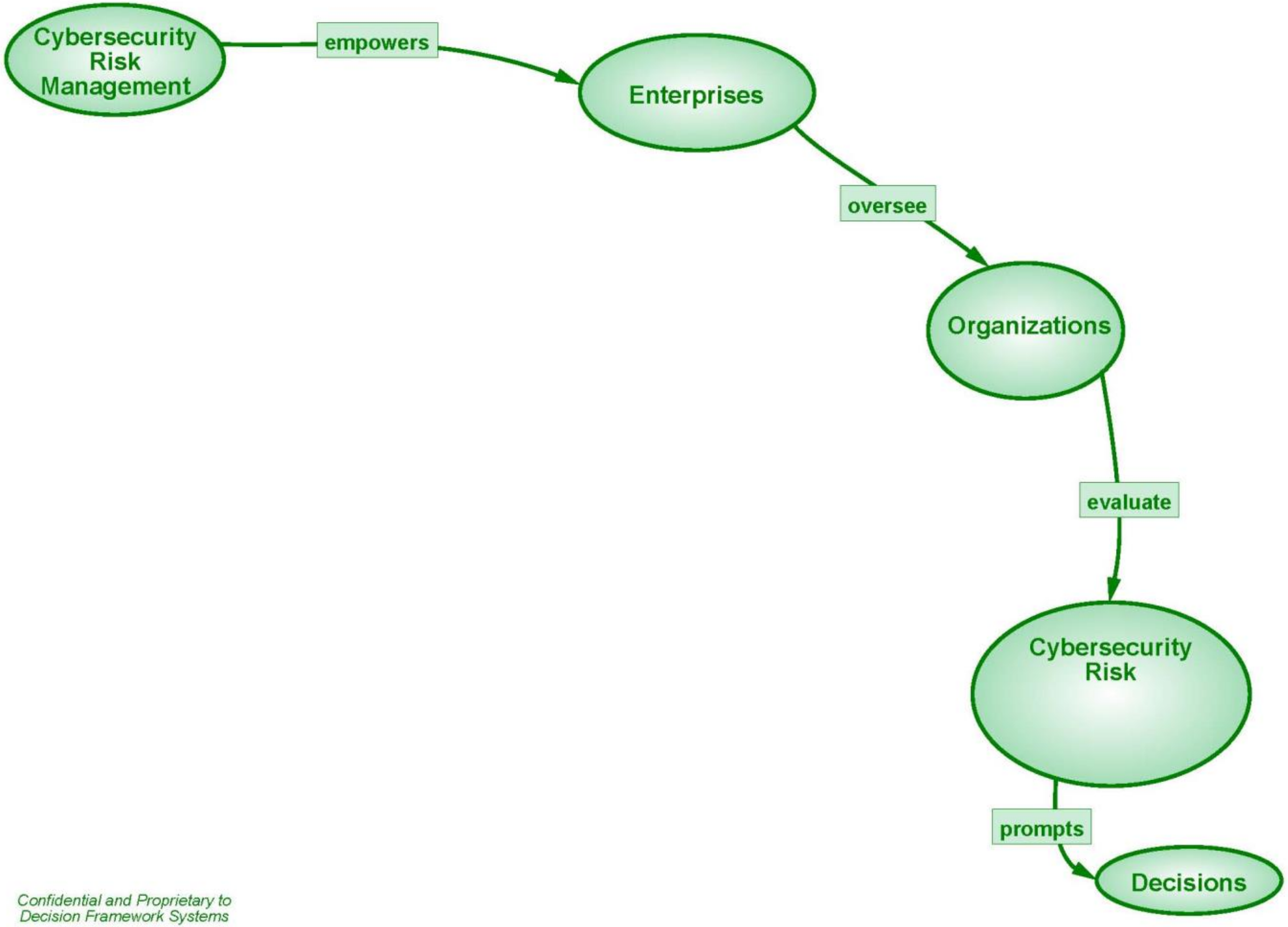
Why not just use FAIR?

Fair provides quantification of potential losses due to known risks but is not a tool for use in situations wherein risks are not well understood. But it is not itself a Framework.



As stated in the FAIR Taxonomy:[*] *"FAIR is complementary to other methodologies like COSO, ITIL, ISO/IEC, 27002:2005, COBIT, OCTAVE, etc. – it provides the engine that can be used in other risk models."*

[*] *Factor Analysis of Information Risk (FAIR), Risk Taxonomy publication, 2009. https://www.fairinstitute.org/*



Cybersecurity Risk Management

empowers

Enterprises

oversee

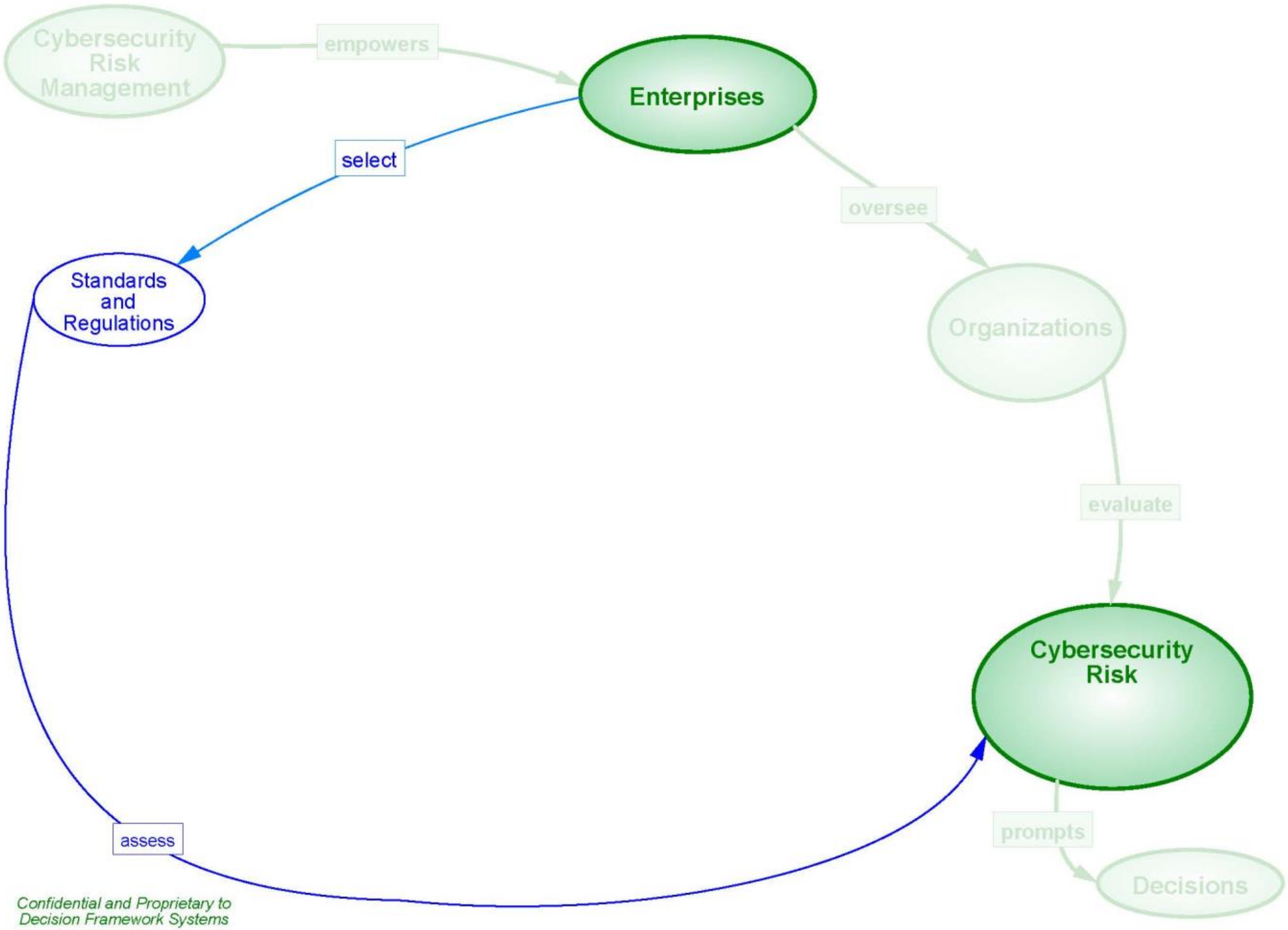
Organizations

evaluate

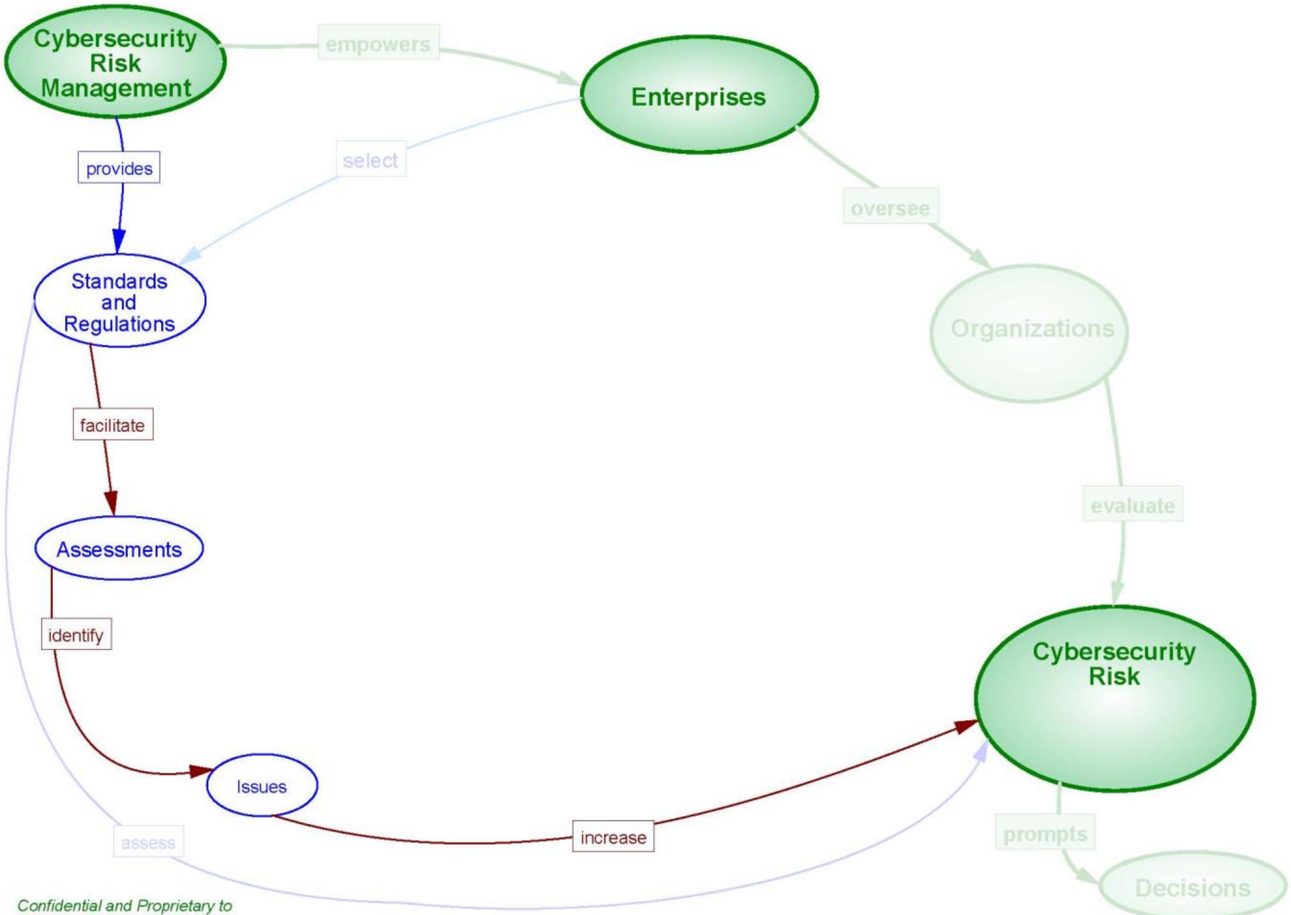
Cybersecurity Risk

prompts

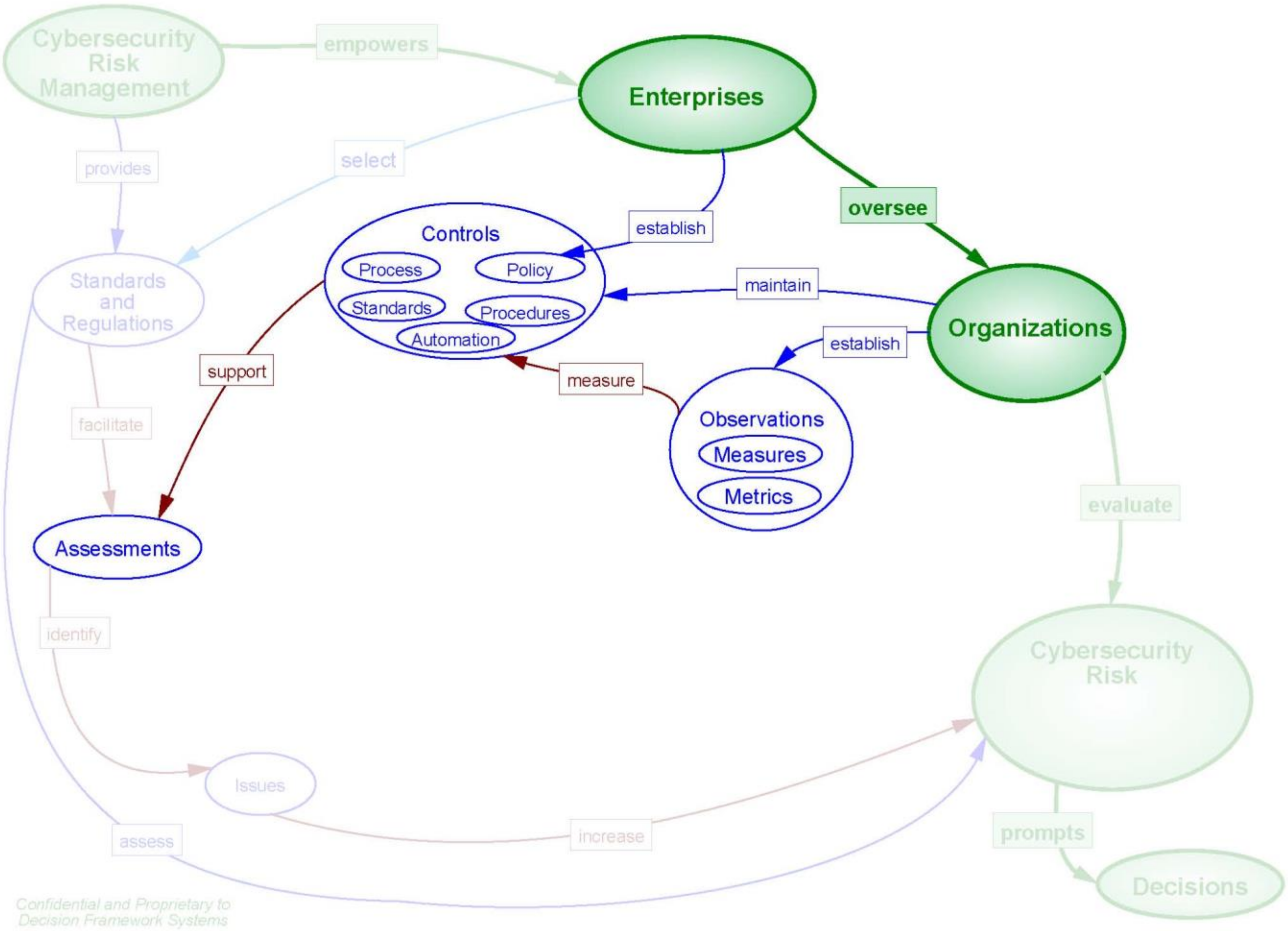
Decisions

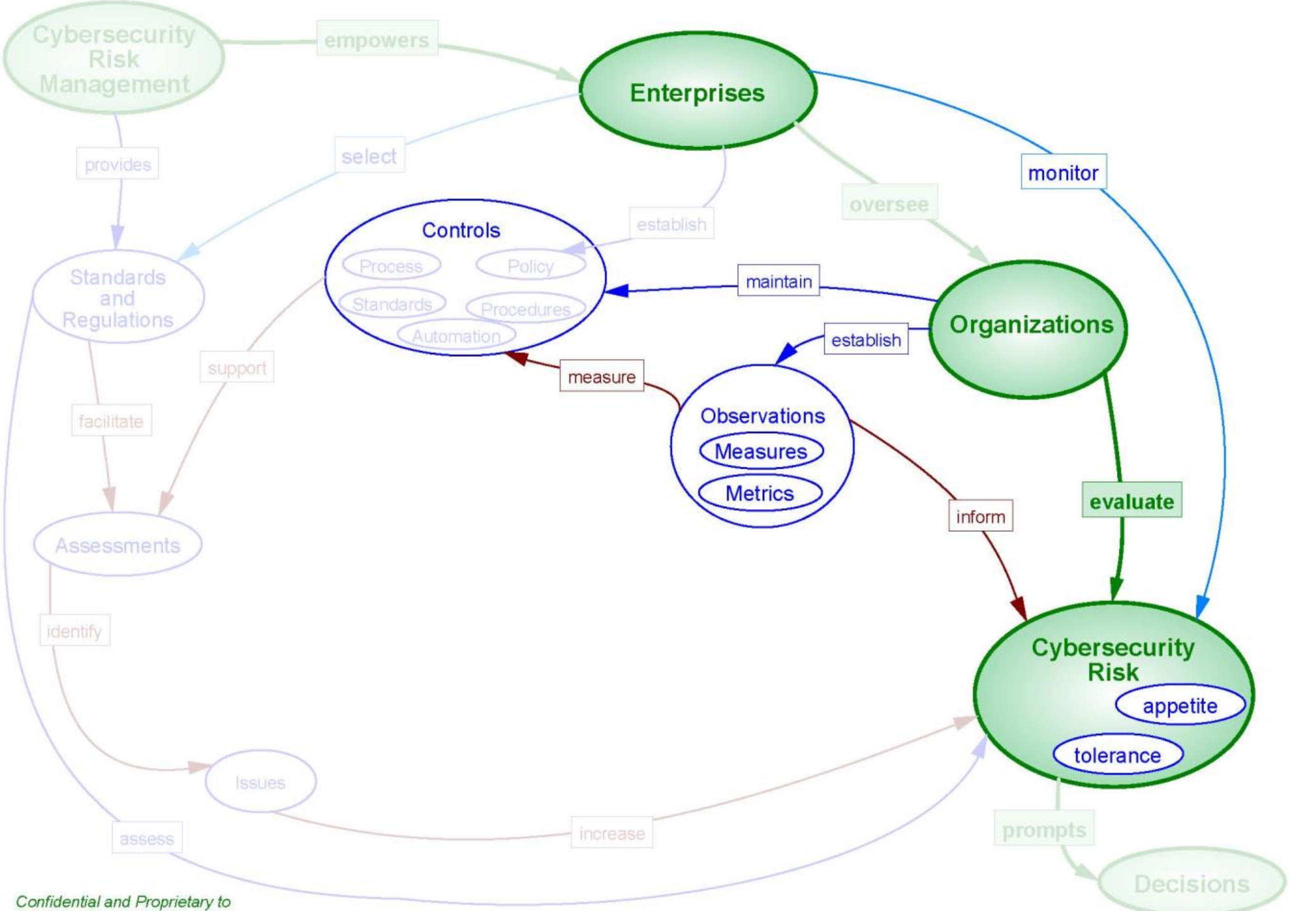


Confidential and Proprietary to Decision Framework Systems

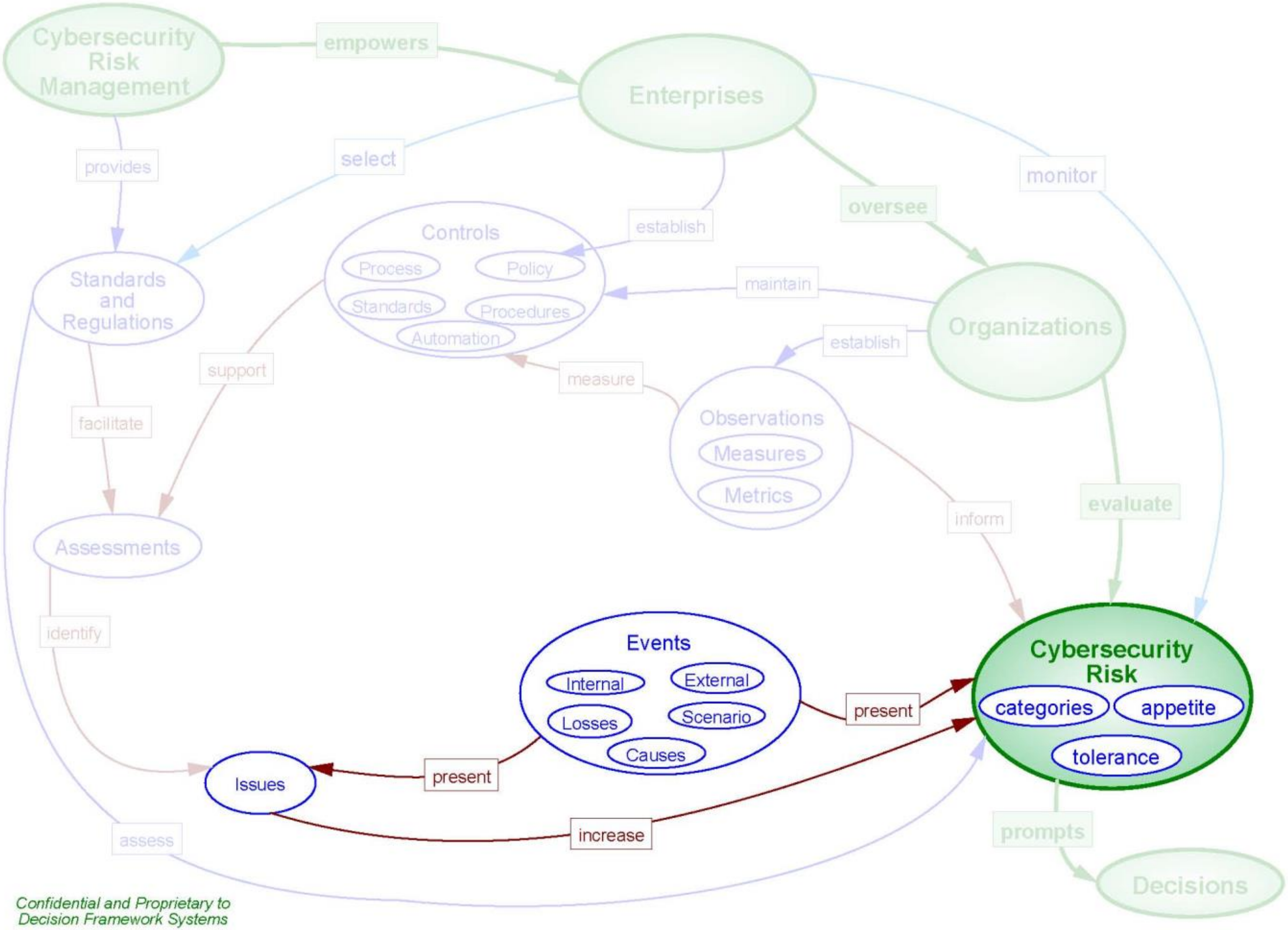


Confidential and Proprietary to Decision Framework Systems

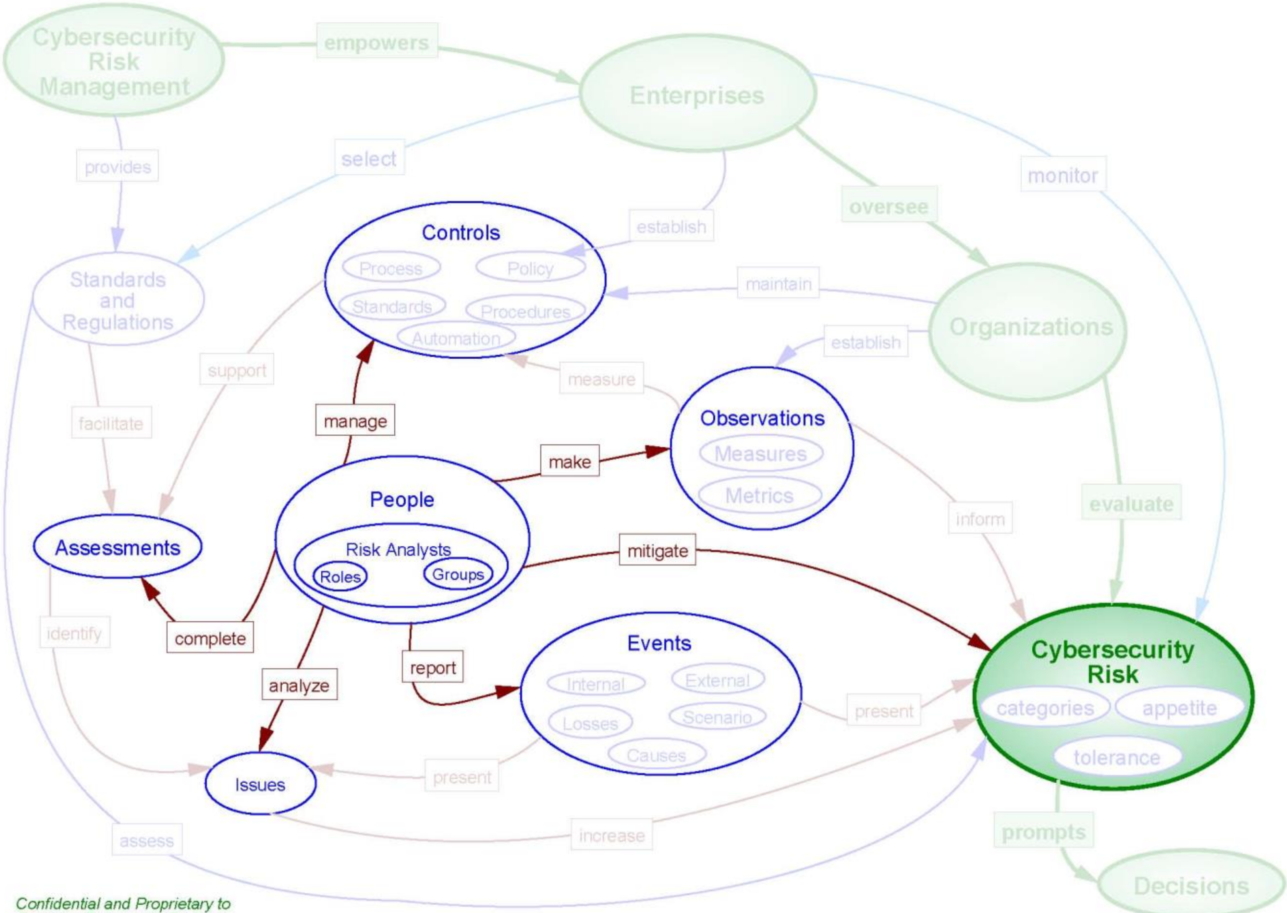

Cybersecurity Risk Management
empowers
Enterprises
provides
select
establish
oversee
Controls
Process
Policy
Standards
Procedures
Automation
maintain
Organizations
establish
Standards and Regulations
support
measure
Observations
Measures
Metrics
facilitate
evaluate
Assessments
identify
Cybersecurity Risk
Issues
increase
assess
prompts
Decisions
Confidential and Proprietary to Decision Framework Systems



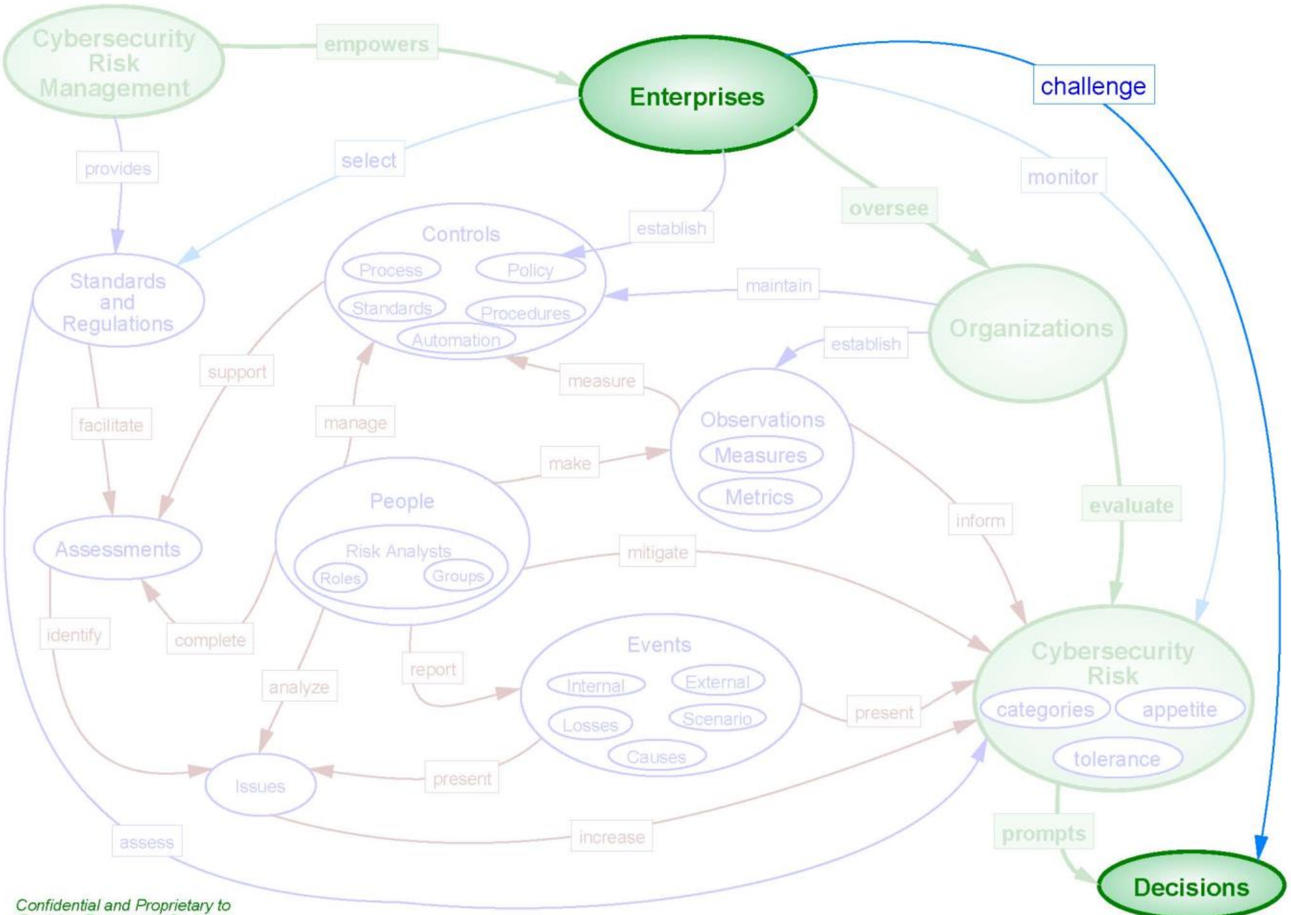
Confidential and Proprietary to Decision Framework Systems



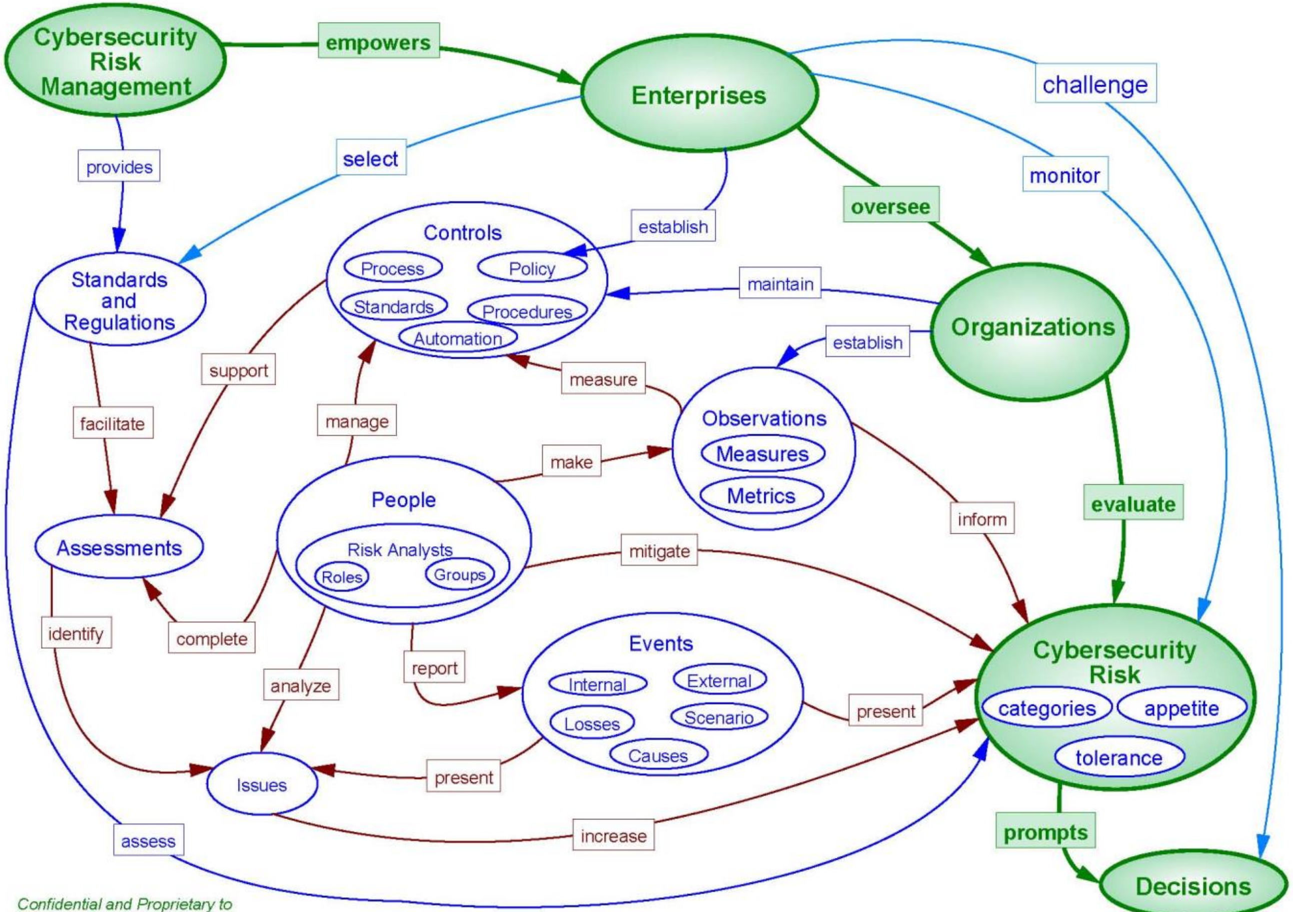
Confidential and Proprietary to Decision Framework Systems



Confidential and Proprietary to Decision Framework Systems

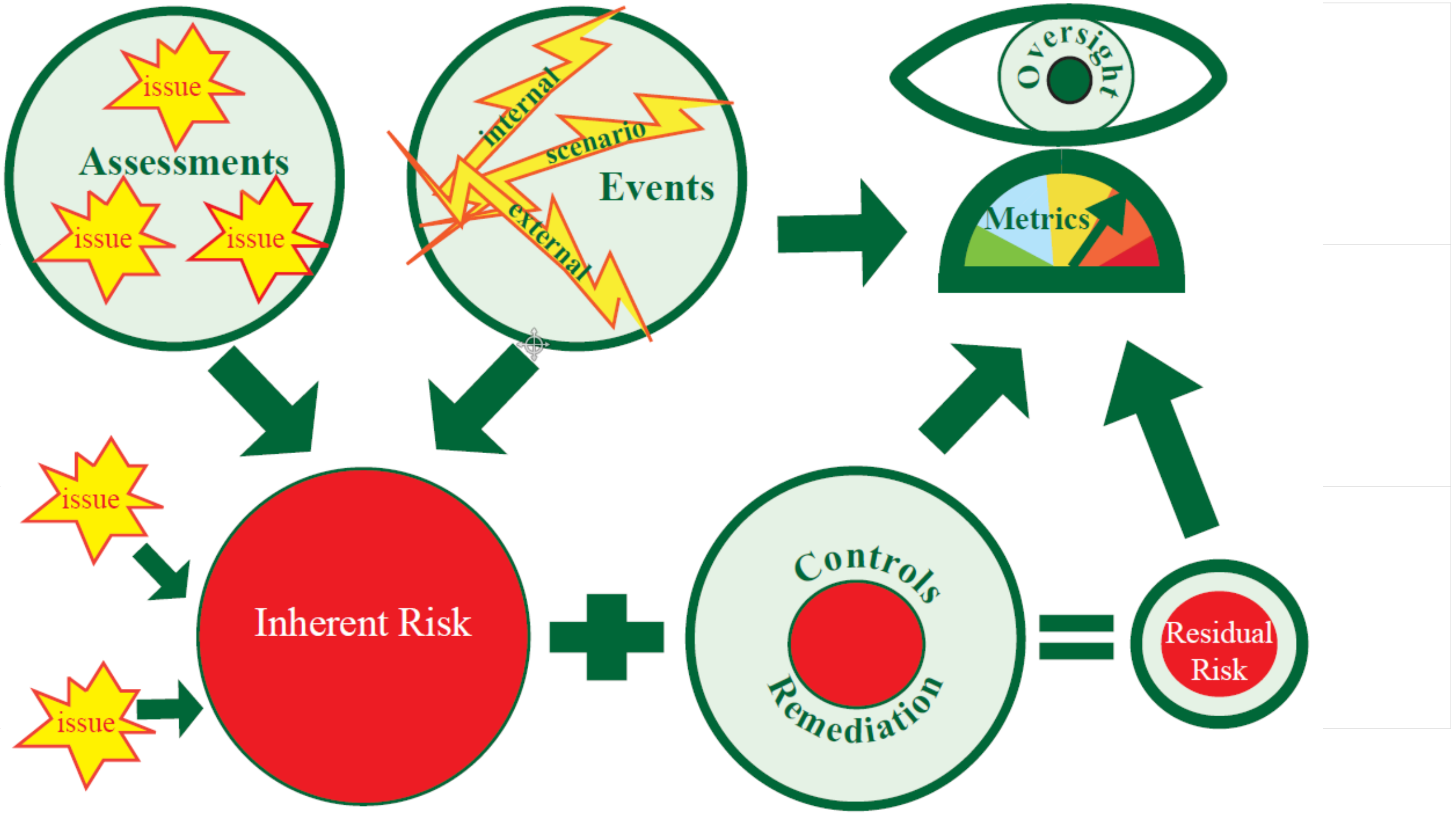


Confidential and Proprietary to
Decision Framework Systems



Confidential and Proprietary to
Decision Framework Systems

Framework Cliff Note Version



Thank you!

Jennifer Bayuk

Decision Framework Systems, Inc.

This presentation has summarized the Framework incorporated in a SaaS product called FrameCyber^{TM}

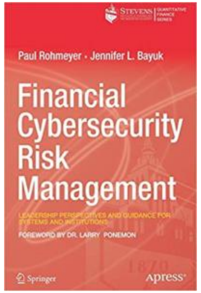
For more information, see the whitepaper at:

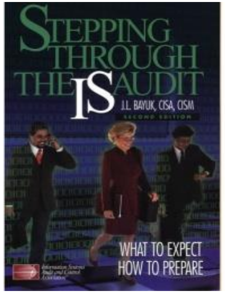
https://kb.framecyber.com/kb/whitepaper?SIRACON

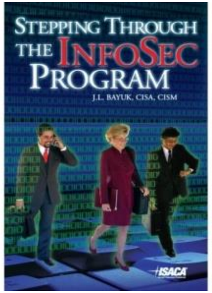
Jennifer Bayuk

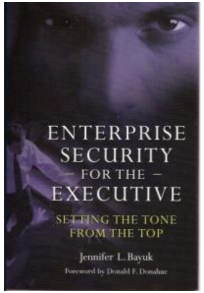
jennifer@bayuk.com

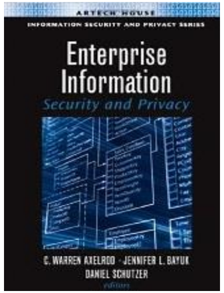
- Experience in a wide variety of private security positions, including Wall Street Chief Information Security Officer, Financial Services Internal Audit, Global Bank Operational Risk Management, and Big 4 Information Systems Risk
- Created curriculum for numerous information security, cybersecurity, and technology risk topics for conferences, seminars, corporate training, and graduate-level programs
- Frequent contributor to Cybersecurity Boards, Committees, and educational forums.
- BS in Computer Science and Philosophy, MS in Computer Science, PhD.
- Author of multiple textbooks and articles on security management topics
- Many publications available for download at: www.bayuk.com

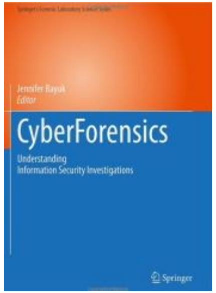

Stevens
Paul Rohmeyer • Jennifer L. Bayuk
Financial Cybersecurity Risk Management
Leadership perspectives and guidance for systems and institutions
Foreword by Dr. Larry Ponemon
Springer
Apress

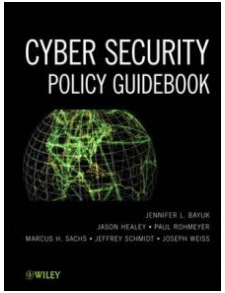





Enterprise Security for the Executive
Setting the Tone from the Top
Jennifer L. Bayuk
Foreword by Donald F. Donahue


Artech House
Information Security and Privacy Series
Enterprise Information Security and Privacy
C. Warren Axelrod • Jennifer L. Bayuk
Daniel Schutzer
editors




Cyber Security Policy Guidebook
Jennifer L. Bayuk
Jason Healey • Paul Rohmeyer
Marcus H. Sachs • Jeffrey Schmidt • Joseph Weiss
Wiley