

Global Risk Management Day

by Copenhagen Compliance*

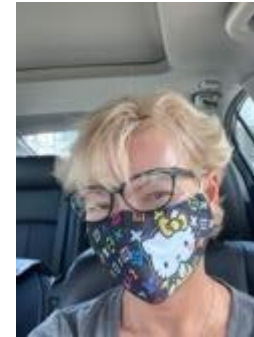
March 11, 2021, Online Conference

Tips to identify threats and vulnerabilities for risk analysis

Lisa Young
VP Cyber Risk Engineering, Axio
Past President, SIRA

Lisa R. Young: collaborative, forward looking, data-driven problem solver

- Product Manager for risk quant SaaS platform development at Axio;
- Mantra: **Cyber Risk Management is a Team Sport!**
- Instructor for Risk Management, Quantitative Risk Analysis, Data Governance, Measuring What Matters: GQIM; BA Business Administration, Marketing; M.Sc., Cybersecurity Public Policy
- Began career in telecommunications and network engineering. Worked in Financial services, Airline, Manufacturing, Automotive & Marine, Telecommunications, Senior Cybersecurity Engineer for CERT at Carnegie Mellon University Software Engineering Institute for 11 years
- SIRA Board President 2017-2020; Past President, VP, and Secretary ISACA West Florida Chapter (2003-2009); ISC2.org Board member (2021-2023)
- Lead author ISACA Risk-IT Framework and Practitioners Guide –the basis for the new **ISACA Risk Fundamentals Certificate**
- LinkedIn email: lyoung@brightmsi.com
- “Lisa Young @ISACA”






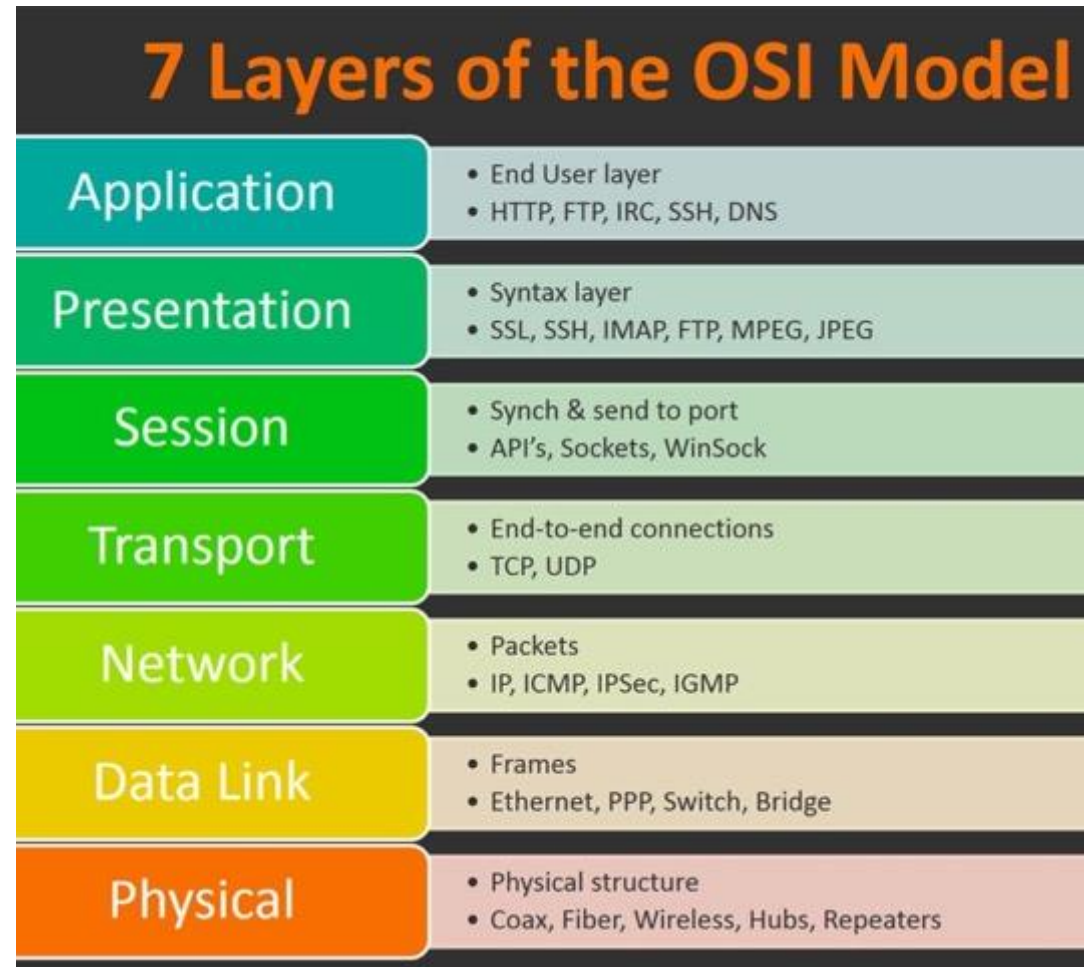
My biases

- I like heat maps as a visualization tool – provided there is some rigor to the underlying analysis as to why the risk is in a certain “box.”
- I believe risk analysis should be performed in relation to a business problem, a question to be answered, or a desired outcome.
- I have an extensive background in cyber-physical (transportation, healthcare, manufacturing) and organizational dependencies/supply chain risk (energy, water, telecom) and think that it gets too little attention when creating risk scenarios.

OSI is the basis for all digital communications.

- 
- All
 - People
 - Seem
 - To
 - Need
 - Data
 - Processing

- Away
- Pizza
- Sausage
- Throw
- Not
- Do
- Please



Global Risk Management Day

by Copenhagen Compliance*

March 11, 2021, Online Conference

Setting the context for risk
management

Risk Management

- Definition: Ongoing, proactive process of adopting a holistic approach to address uncertainty which:
 - may affect the achievement of business or enterprise objectives
 - leads to greater business robustness and resilience (minimizes downside impact)
 - enables efficient risk-taking for appropriate benefit (opportunity)

Establish repeatable process to minimize and mitigate loss

Risk Types

Enterprise Risk

Strategic
Risk

Environmental
Risk

Market
Risk

Credit
Risk

Operational
Risk

Compliance
Risk

I&T-related Risk

I&T Benefit/Value
Enablement Risk

IT Program
Project-delivery Risk

IT Operations and
Service-delivery Risk

Cyber and Information
Security Risk

Any difference in Cyber Risk?

Cyber

Of or relating to computers, information technology, electronic communications (especially the internet), or virtual reality

Risk

Exposure to danger, harm, or loss

Cyber Risk

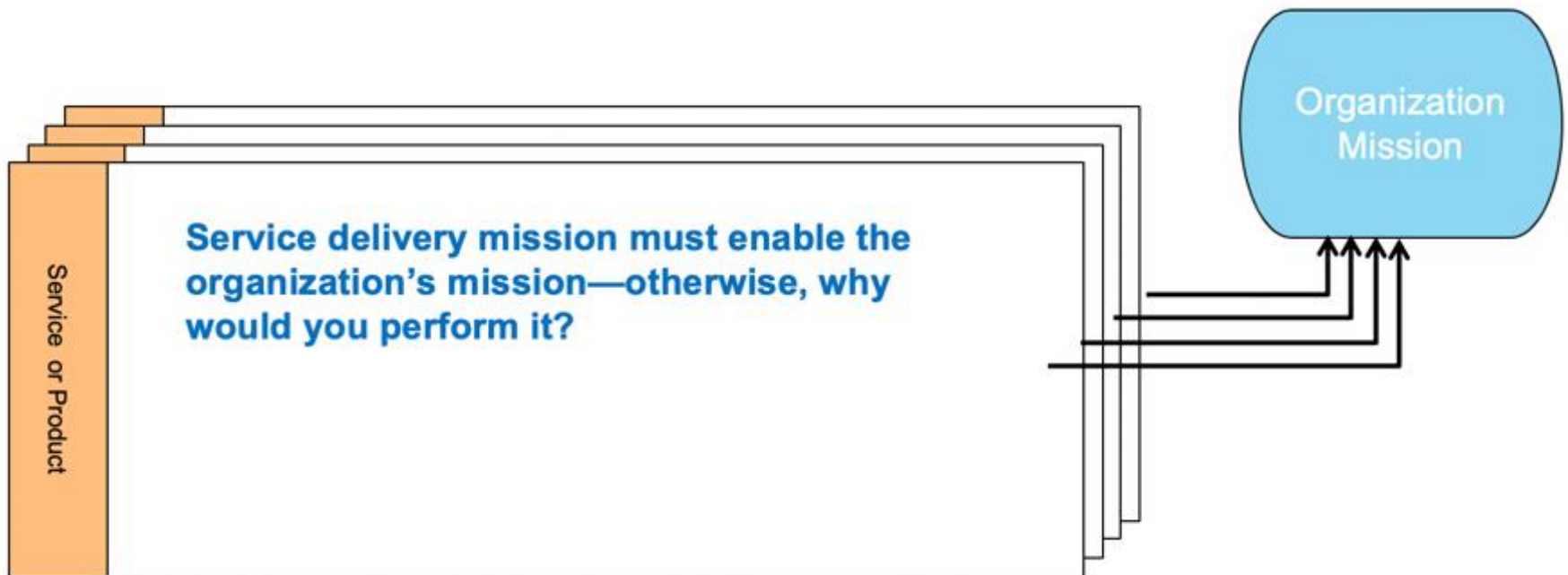
Exposure to danger, harm, or loss **related to the use of or dependence on computers, electronic data, or electronic communications** (including the internet)

Typically involves unauthorized access or unauthorized use of computer technology

Cyber risk increases as our dependence on computer technology accelerates

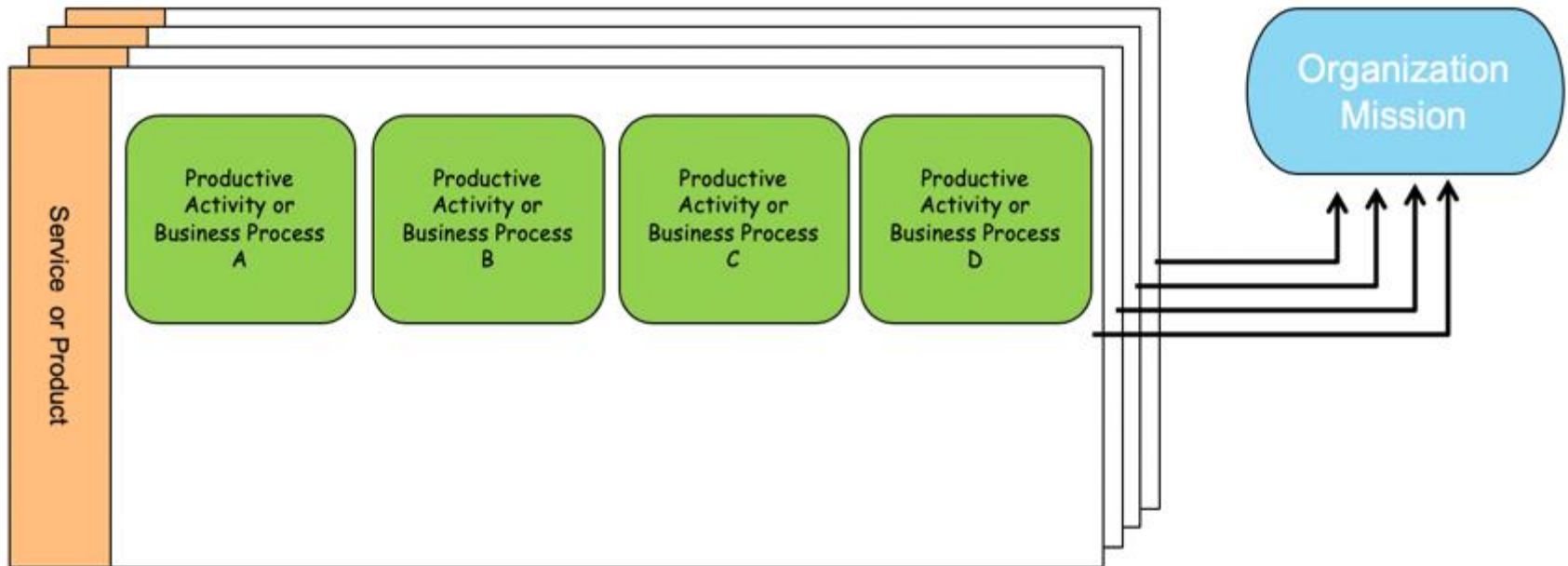
Enterprise Services, Products, Mission

- Outputs of an organization
- Can be internally or externally focused
- Typically align with a specific organizational unit, but can cross units and organizational boundaries
- Collectively they enable an organization's mission



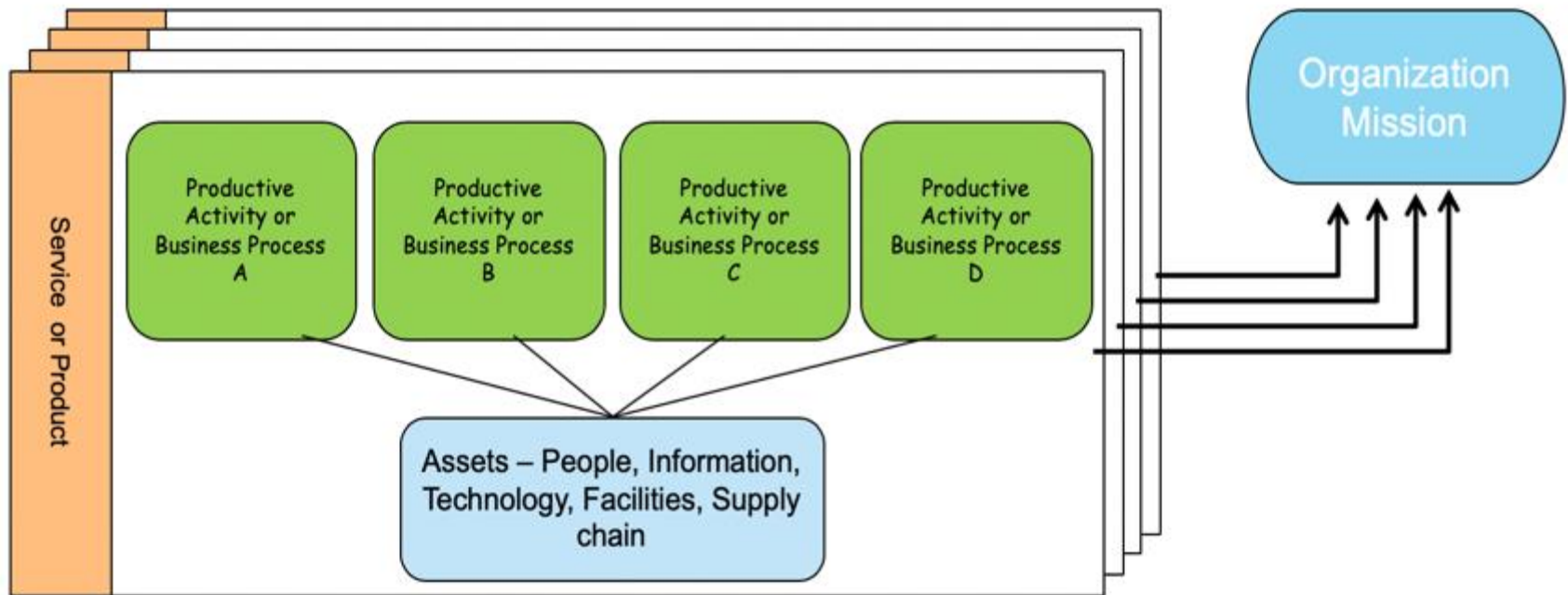
Business Operations, Business Processes, Productive Activities, Projects, Initiatives

- The activities that the organization (and/or its suppliers) perform to ensure that services and products are produced
- Traverse the organization; cross organizational lines
- A service or a product is made up of one or more Business Processes, productive activities, projects or whatever they are called in your organization.

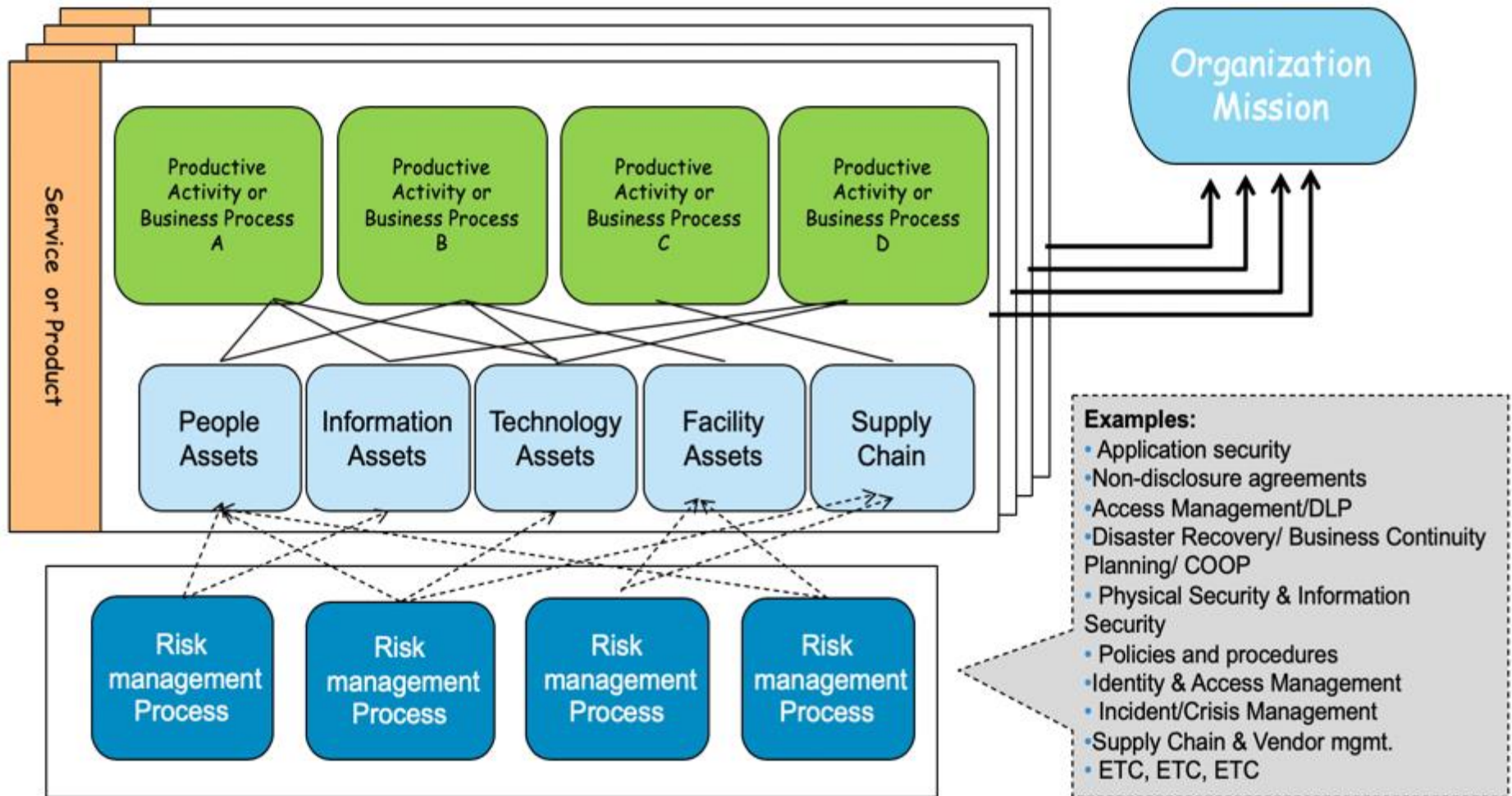


Assets

- Something of value to the organization
- Placed into production to deliver and support services
- Asset value relates to the importance of the asset in meeting the enterprise mission.



Organizational Context for Risk



Where does Risk Analysis and Business Impact Evaluation fit in Risk Management



Global Risk Management Day

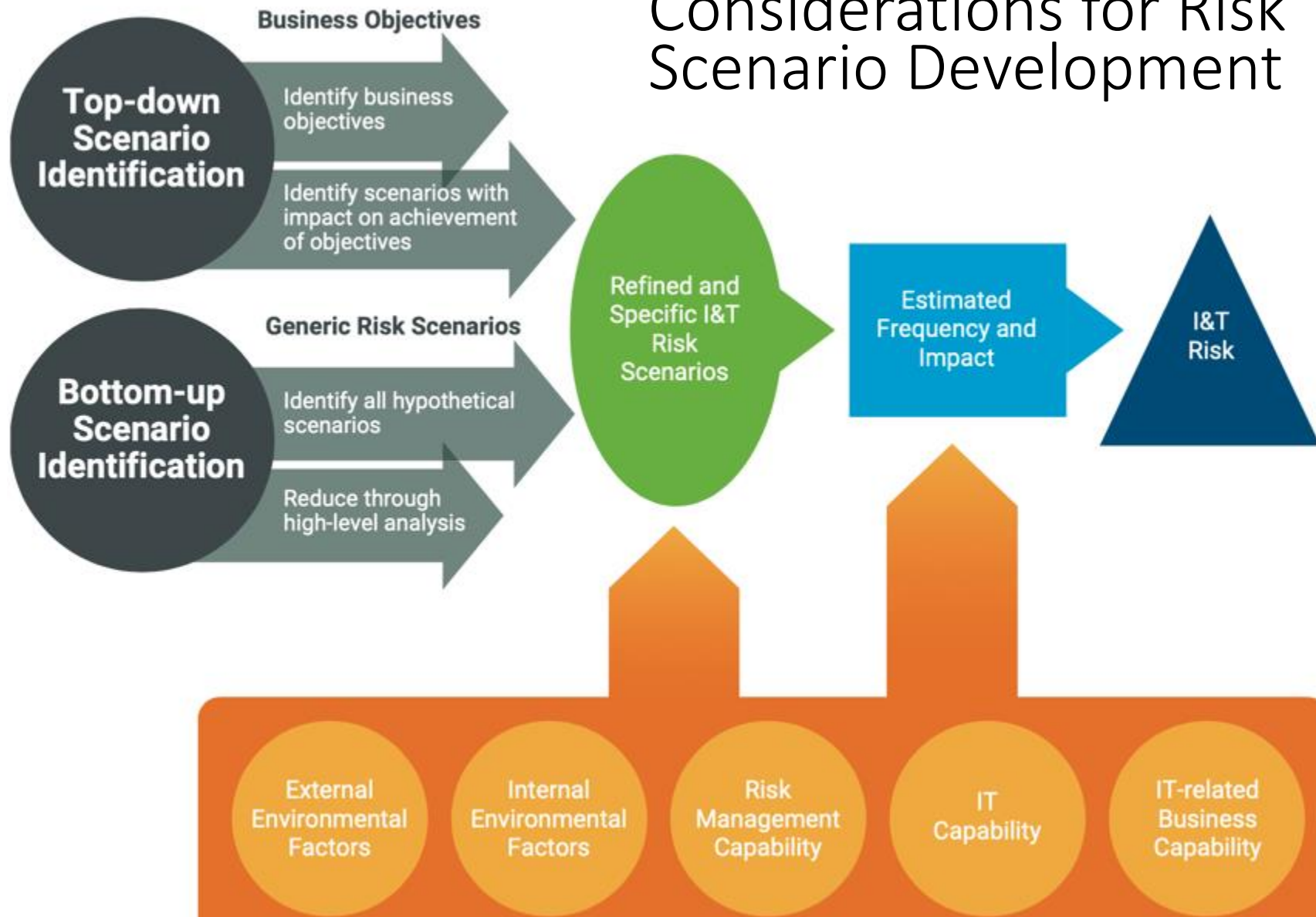
by Copenhagen Compliance*

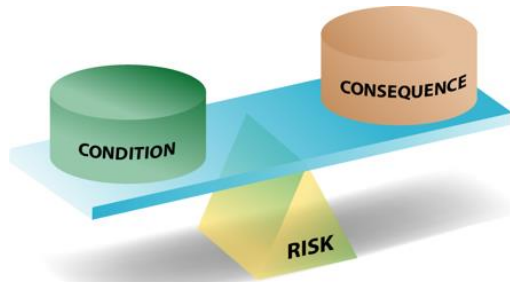
March 11, 2021, Online Conference

Inputs to Scenario Analysis

Tips to identify threats and vulnerabilities

Considerations for Risk Scenario Development



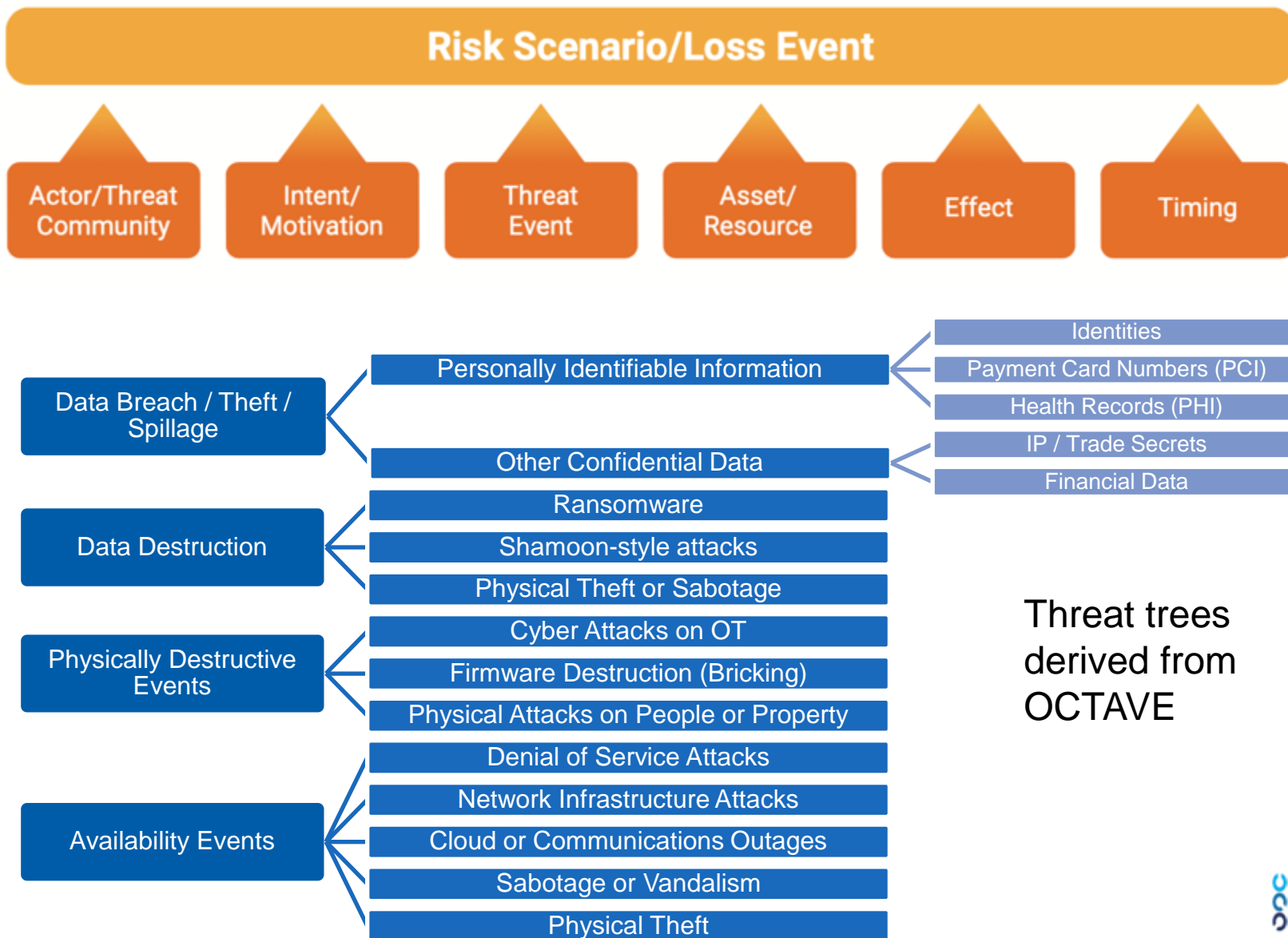


Enterprise goals and objectives
Strategic importance of IT for the business
Complexity of IT
Complexity of the entity and degree of change
Change management capability
Operating model
Strategic priorities
Culture of the enterprise
Financial capacity

Market and economic factors
Rate of change in the market/product life cycle
Industry and competition
Geopolitical situation
Regulatory environment
Technology status and evolution
Threat landscape

Conditions and Consequences

Considerations for threats and vulnerabilities as inputs to loss events



VERIS Taxonomy High-Level



VERIS - <http://veriscommunity.net/veris-overview.html>

A TAXONOMY OF THREATS FOR COMPLEX RISK MANAGEMENT



University of Cambridge Centre for **Risk Studies**

- *...taxonomy of macro-catastrophe threats that have the potential to cause damage and disruption to social and economic systems in the modern globalized world.*
- Contains
 - 5 Primary Classes
 - 11 Families
 - 55 (Genus) Types
- Very high level

Operational Risk Taxonomy

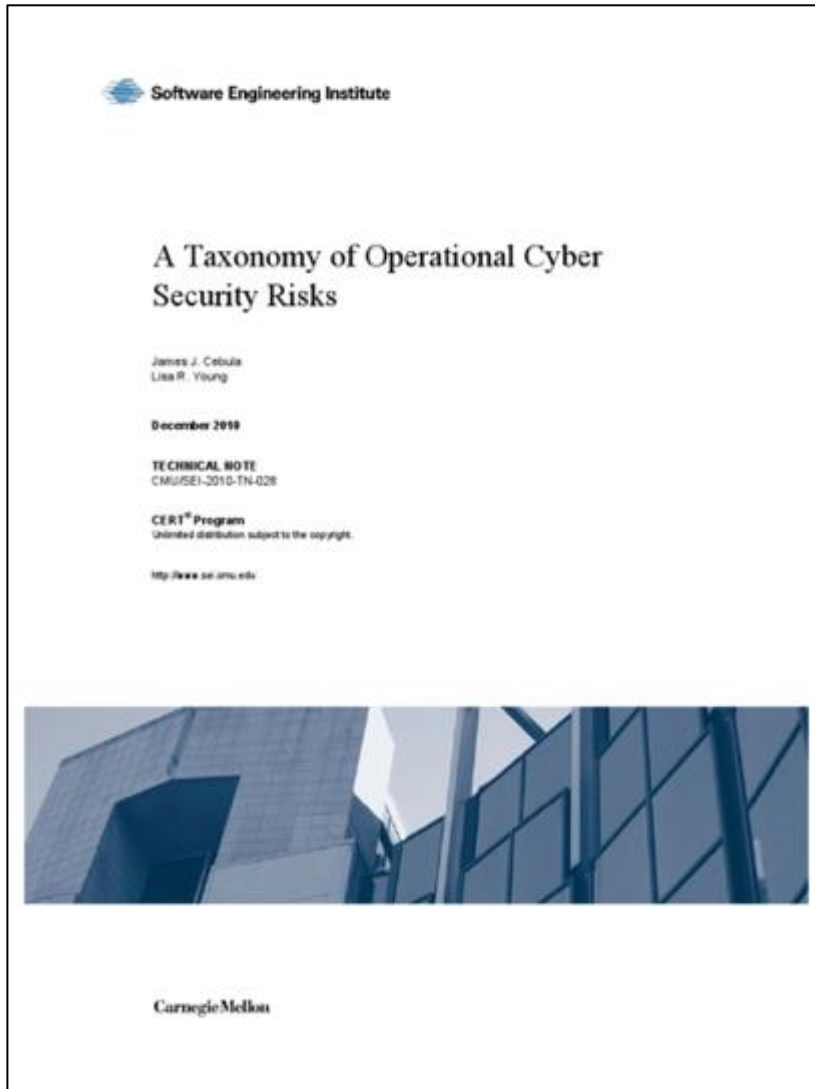


Table 1: Taxonomy of Operational Risk

1. Actions of People	2. Systems and Technology Failures	3. Failed Internal Processes	4. External Events
1.1 Inadvertent 1.1.1 Mistakes 1.1.2 Errors 1.1.3 Omissions 1.2 Deliberate 1.2.1 Fraud 1.2.2 Sabotage 1.2.3 Theft 1.2.4 Vandalism 1.3 Inaction 1.3.1 Skills 1.3.2 Knowledge 1.3.3 Guidance 1.3.4 Availability	2.1 Hardware 2.1.1 Capacity 2.1.2 Performance 2.1.3 Maintenance 2.1.4 Obsolescence 2.2 Software 2.2.1 Compatibility 2.2.2 Configuration management 2.2.3 Change control 2.2.4 Security settings 2.2.5 Coding practices 2.2.6 Testing 2.3 Systems 2.3.1 Design 2.3.2 Specifications 2.3.3 Integration 2.3.4 Complexity	3.1 Process design or execution 3.1.1 Process flow 3.1.2 Process documentation 3.1.3 Roles and responsibilities 3.1.4 Notifications and alerts 3.1.5 Information flow 3.1.6 Escalation of issues 3.1.7 Service level agreements 3.1.8 Task hand-off 3.2 Process controls 3.2.1 Status monitoring 3.2.2 Metrics 3.2.3 Periodic review 3.2.4 Process ownership 3.3 Supporting processes 3.3.1 Staffing 3.3.2 Funding 3.3.3 Training and development 3.3.4 Procurement	4.1 Disasters 4.1.1 Weather event 4.1.2 Fire 4.1.3 Flood 4.1.4 Earthquake 4.1.5 Unrest 4.1.6 Pandemic 4.2 Legal issues 4.2.1 Regulatory compliance 4.2.2 Legislation 4.2.3 Litigation 4.3 Business issues 4.3.1 Supplier failure 4.3.2 Market conditions 4.3.3 Economic conditions 4.4 Service dependencies 4.4.1 Utilities 4.4.2 Emergency services 4.4.3 Fuel 4.4.4 Transportation

Maps to 800-53r4 and supports the Basel definition of Operational Risk

Building a Risk Taxonomy

1. Get management commitment and collaborate with ERM (if applicable)
2. Design the form of the taxonomy (which could evolve during development)

3. Top-down approach

- a. Gather risk information from various sources, include threat and vulnerability information
- b. Study risk events that have impacted other organizations like yours
- c. Review generic risk taxonomies
- d. Identify high level categories of risk that are relevant to your organization
- e. Add risk categories to your risk register contents

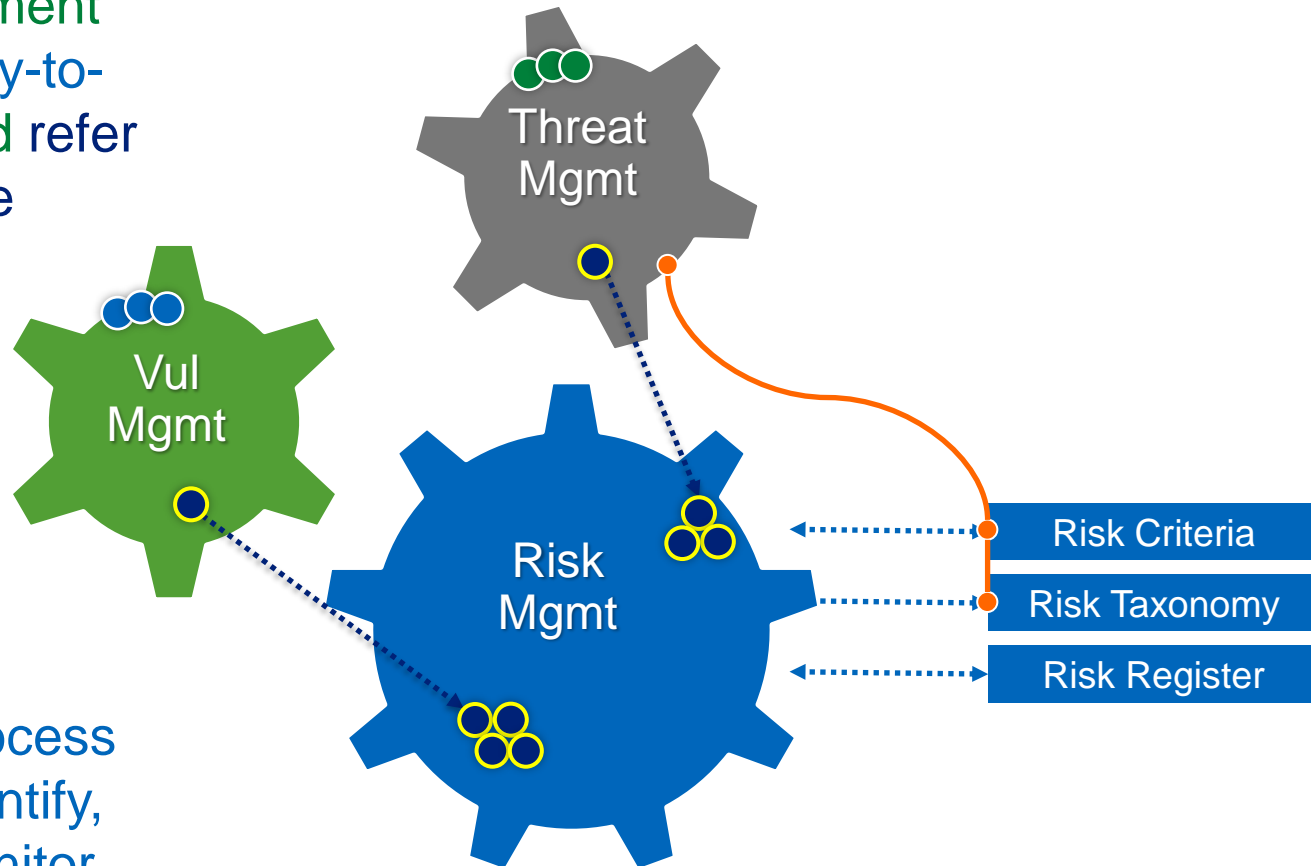
4. Bottom-up approach

- a. Perform an affinity grouping from all risks in your risk register
- b. Use the affinity groups as the high level categories of risk in your risk taxonomy
- c. Add risk categories to your risk register contents

Using both the top-down and bottom-up techniques might improve confidence in the categories and the identified risks

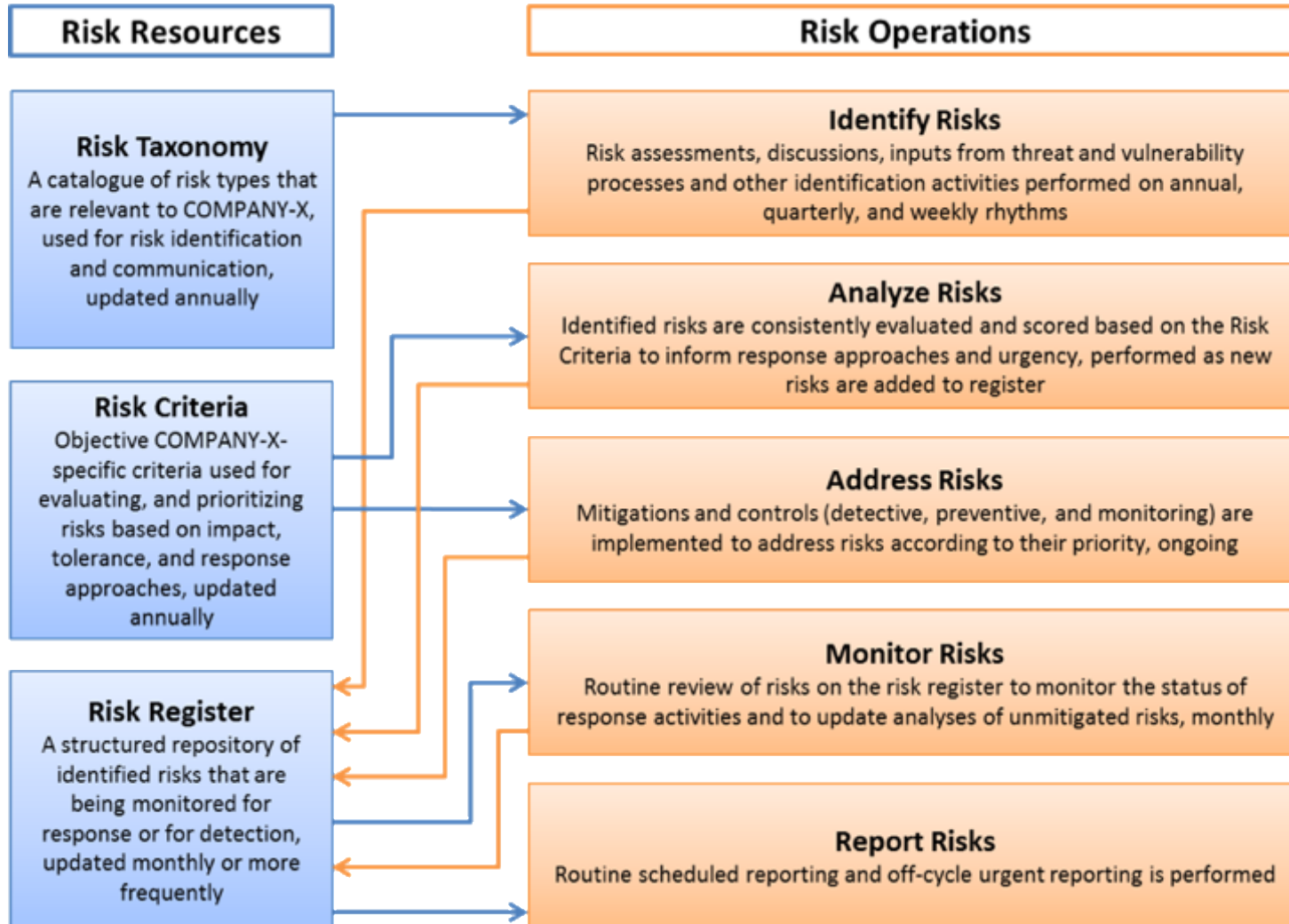
Risk Ecosystem

Vulnerability Management process deals with day-to-day vulnerabilities and refer others to Risk or Issue Management



Risk Management process should continually identify, analyze, address, monitor, and report risks

Holistic view of the Risk Management Process, of which quantitative analysis is one part



Summary

- Building a risk quantification method or program is by definition “measuring” something.
- There are foundational elements that need to be in place for a successful risk quantification program:
 - Business objectives and goals
 - Method and program
 - A set of questions that can be answered with the data; “clean” data
 - Process and workflow; roles and responsibilities
 - Results that are generated from data – minimizes “gaming” and provides context to compare results.
 - Governance and oversight of the method and program





Questions?

- Lisa Young
lyoung@brightmsi.com