



CYBER SECURITY

Ponce Garcia Roberto

Reveles Ariadne S

Ornelas Maria G



Esta foto de Autor desconocido está bajo licencia [CC BY-ND](#)



Esta foto de Autor desconocido está bajo licencia [CC BY-ND](#)

WHY CYBER SECURITY??

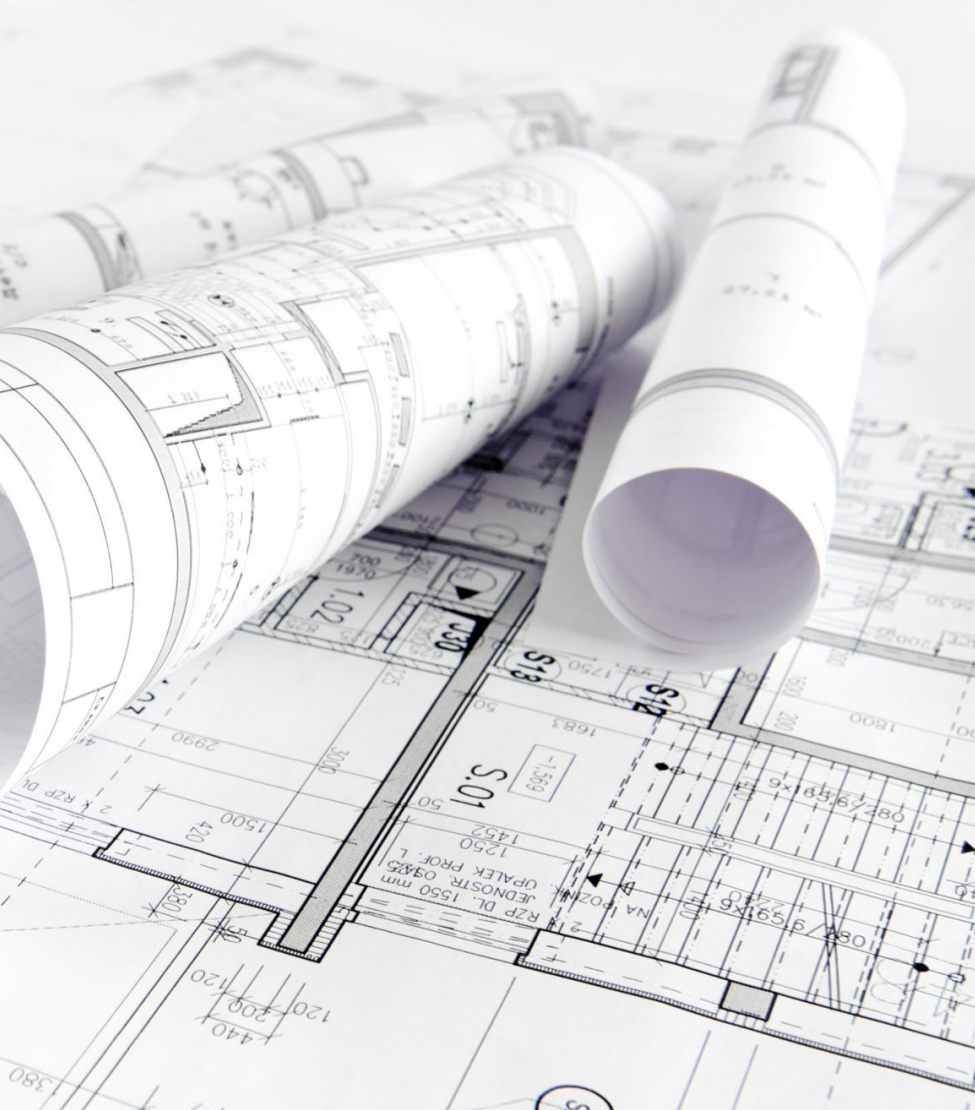
- ❖ Almost one-third of U.S. businesses reported experiencing a breach within this past year.
- ❖ The average cost per data breach in 2017 was in excess of \$3 million USD — with the average number of compromised records per breach rising to 24,000.
- ❖ In 2017, the average time it took an organization to identify a data breach was a little over six months: 191 days, to be precise.

PROJECT GOALS

GENERATE A ROBUST ARCHITECTURE FOR
INFORMATION SECURITY

PROBLEM STATEMENT

1. External hacking attempts
2. Third-party risks
3. Data loss



WHAT IS SYSTEMS ENGINEERING

- Systems Engineering is a transdisciplinary and integrative approach to enable the successful realization, use, and retirement of engineered systems, using systems principles and concepts, and scientific, technological, and management methods.

SYSTEM ENGINEERING FOCUS ON:

Establishing,
balancing
and
integrating

Establishing, balancing and integrating stakeholders' goals, purpose and success criteria.

Establishing

Establishing an appropriate lifecycle model, process approach and governance structures

Generating
and
evaluating

generating and evaluating alternative solution concepts and architectures.

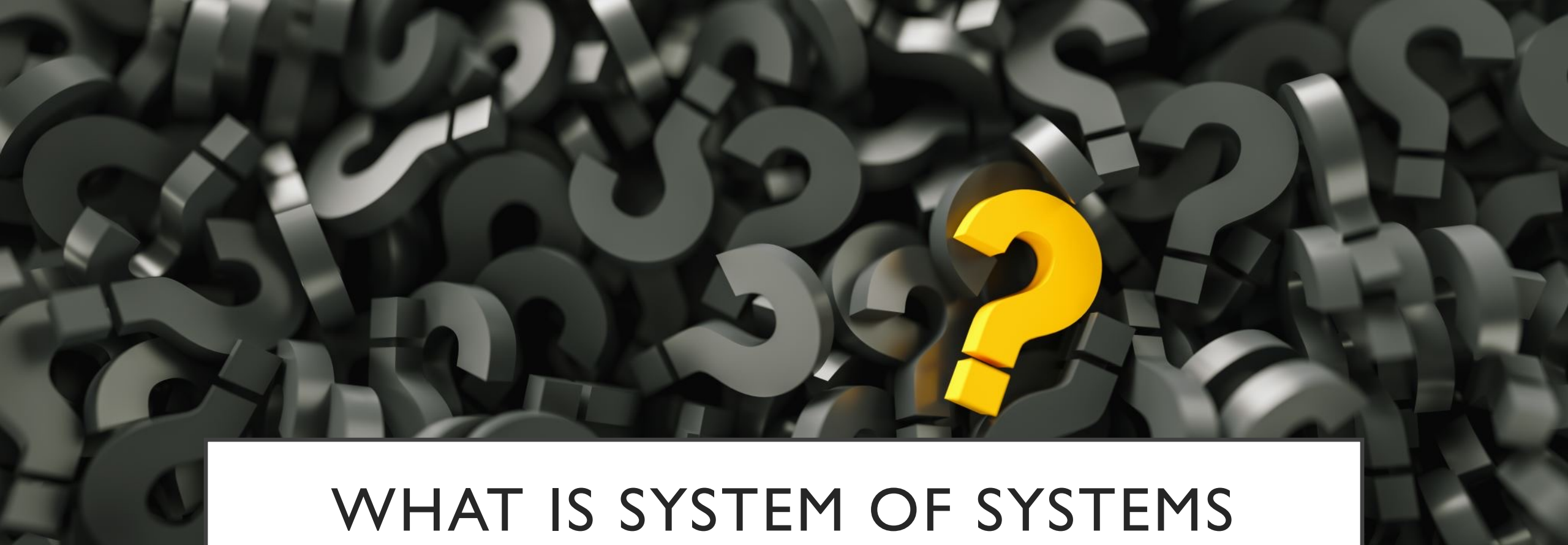


HOW IS SE
APPLICABLE
IN CYBER
SECURITY?

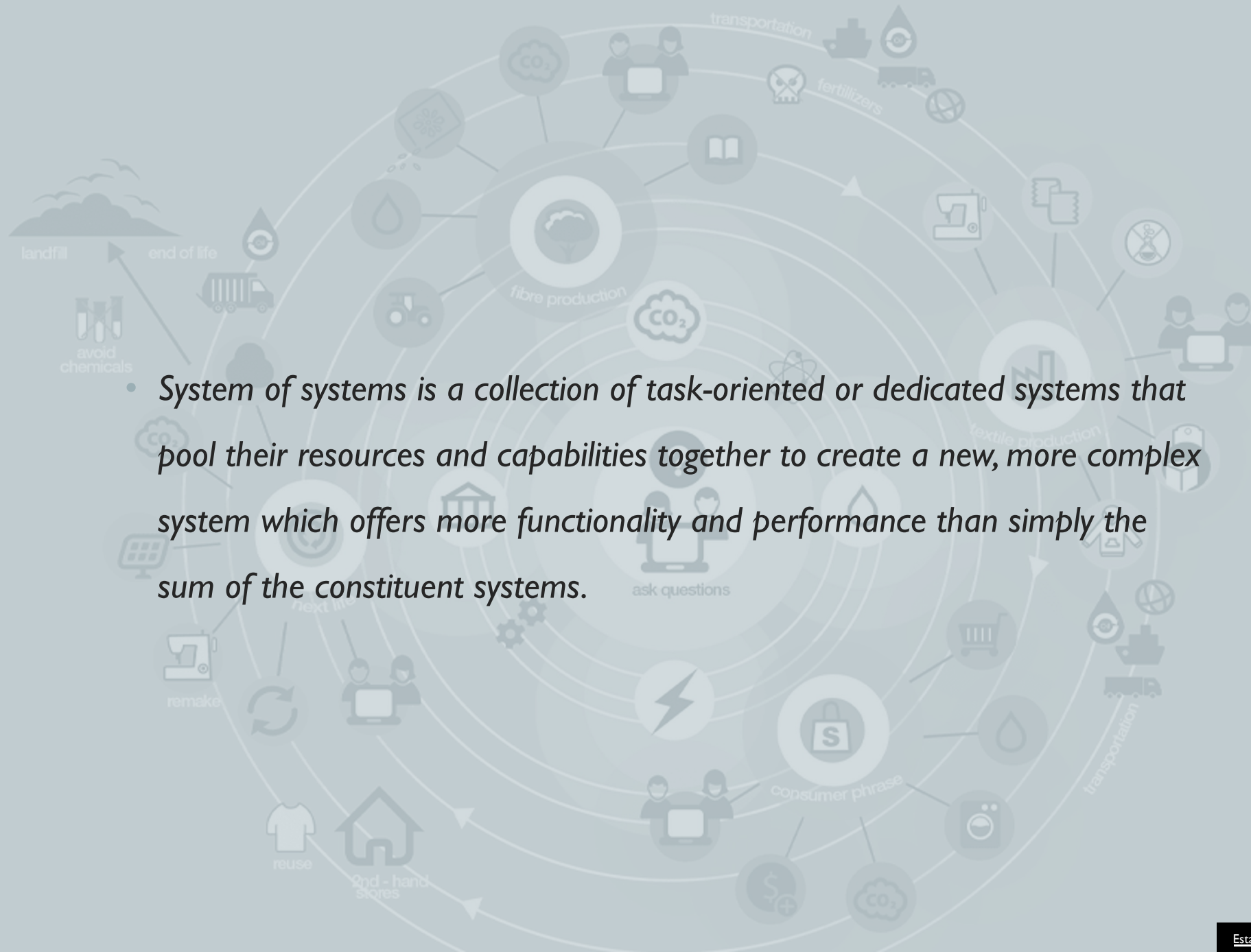
Systems engineering techniques can help protect the by building a cyber security architecture combining the already established CIA TRIAD with DoDaF 2.0

CAPABILITY REQUIREMENTS FOR THE SYSTEM

1. **Confidentiality**
2. **Availability**
3. **Integrability**



WHAT IS SYSTEM OF SYSTEMS
(SOS)?



- *System of systems is a collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new, more complex system which offers more functionality and performance than simply the sum of the constituent systems.*

DODAF 2.0

DEPT. of DEFENSE ARCHITECTURE FRAMEWORK (DoDAF)

VIEWS CONSIST OF:

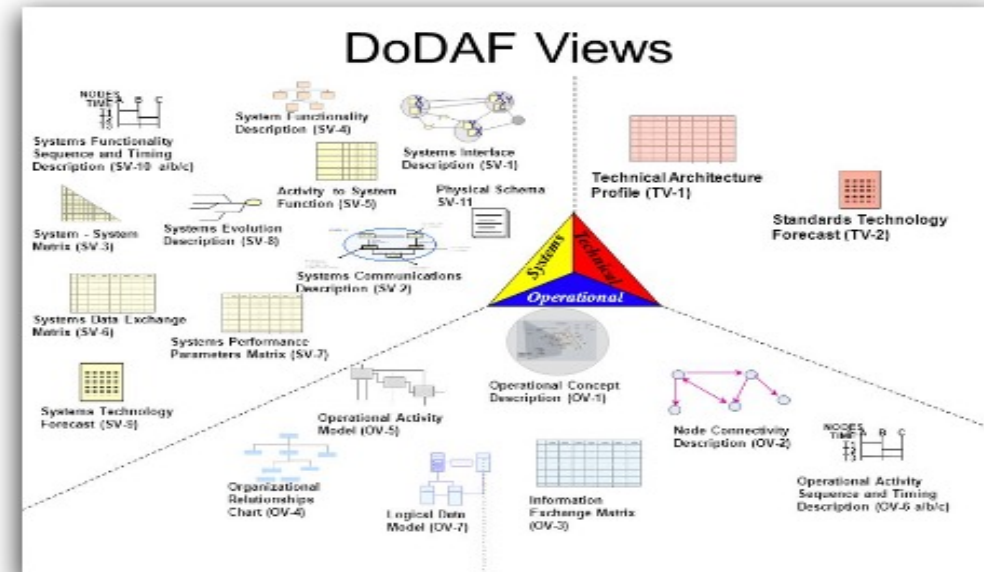
- Operational Views (OV)
- System Views (SV)
- Technical Views (TV)
- All Views (AV) = Combo of OV + SV + TV

PROVIDES INFORMATION ABOUT:

- Structure of SYSTEMS involved in an org for MANY LAYERS of abstraction.

★ MUST BE FOLLOWED BY:

- Organization doing govt. work
- Govt. contract work



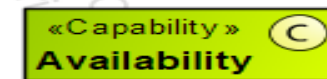
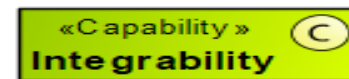
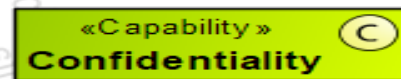
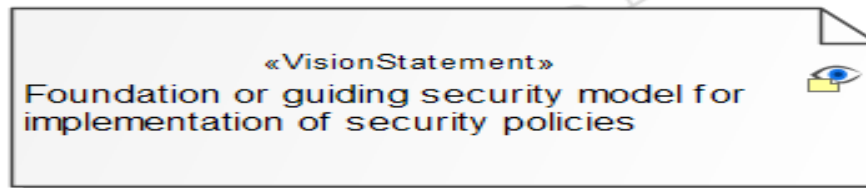
THE CIA TRIAD

CIA TRIAD | **CONFIDENTIALITY** + **INTEGRITY** + **AVAILABILITY**



CV-1 VISION

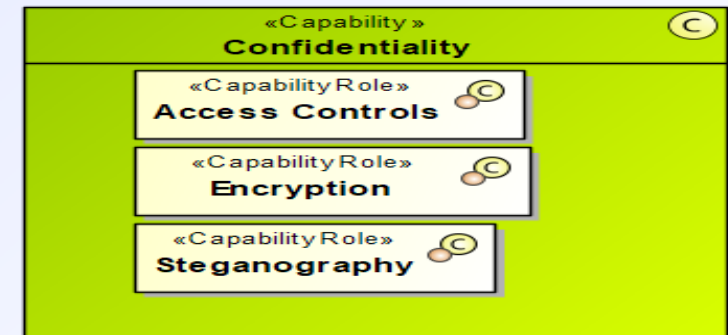
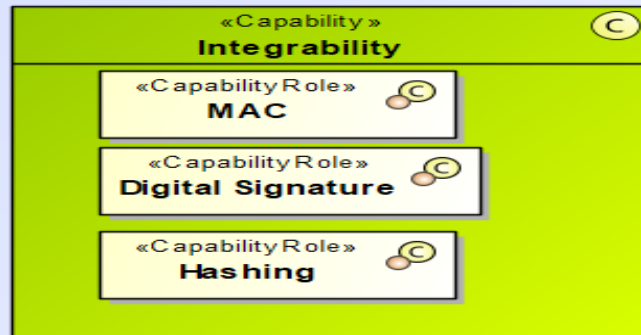
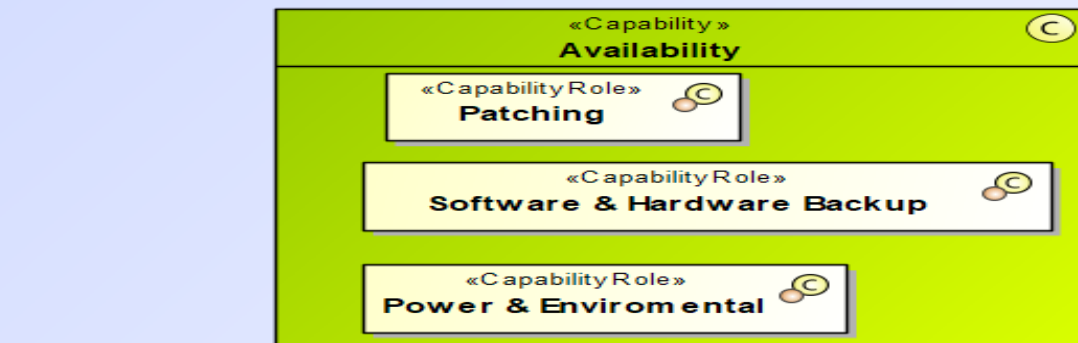
CV-1 Vision [CV-1 Diagram]



CV-2

CV-2 Capability Taxonomy [CV-2 Diagram1]

CV-4



CV-6

Capabilities / Operation	Secure Transfer of Data	User Password/key/hashvalue/MAC	Backups IT Engineer	Maintenance of Power Sources	Cyber Security Engineer
Confidentiality	X	X	X		X
Integrability	X	X	X		X
Availability	X	X	X	X	

CV-7

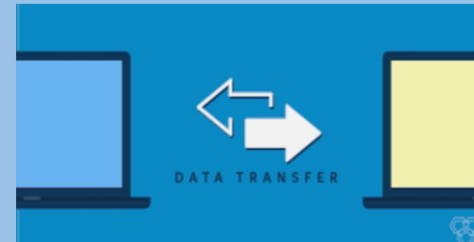
Capabilities / Operation	Hardware/Software/Storage Recovery	Authorization & Authentication	Protection of Data	Network Security	Power Restoration & Backup
Confidentiality		X	X	X	
Integrability		X	X		
Availability	X	X	X	X	X

OV-I

OV-1 High Level Operational Concept Graphic



Data Backup

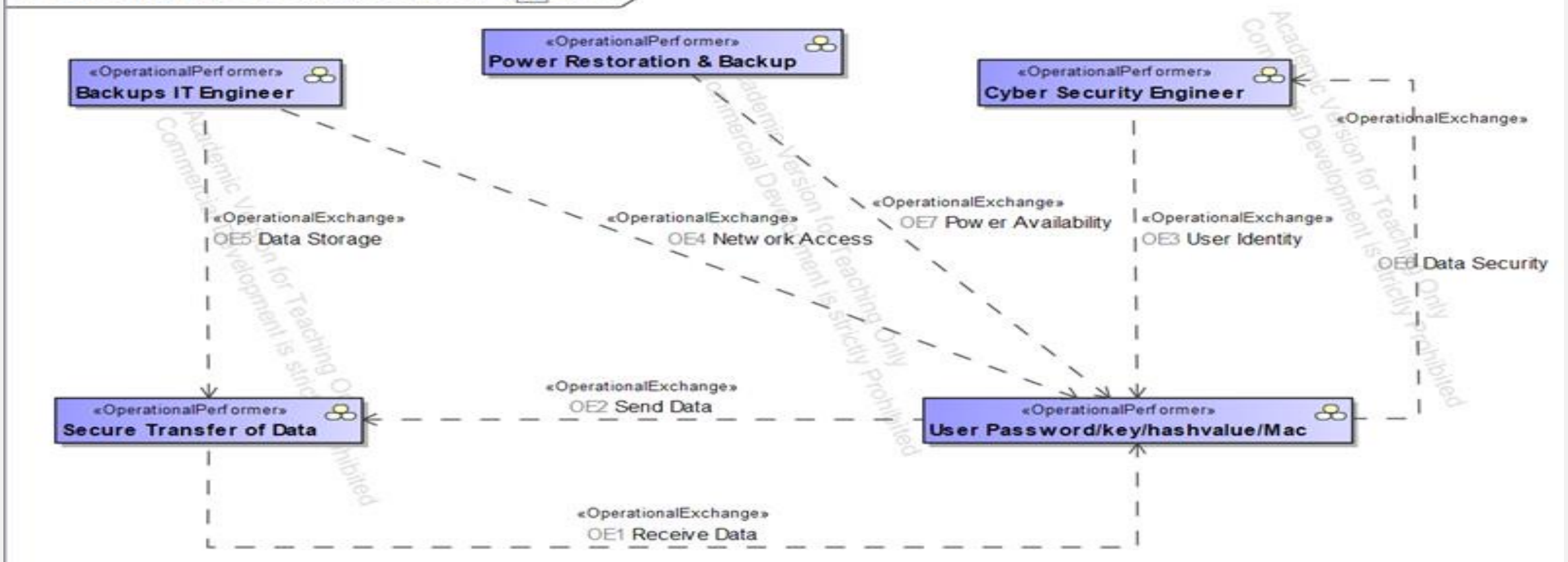


Verification of Identity



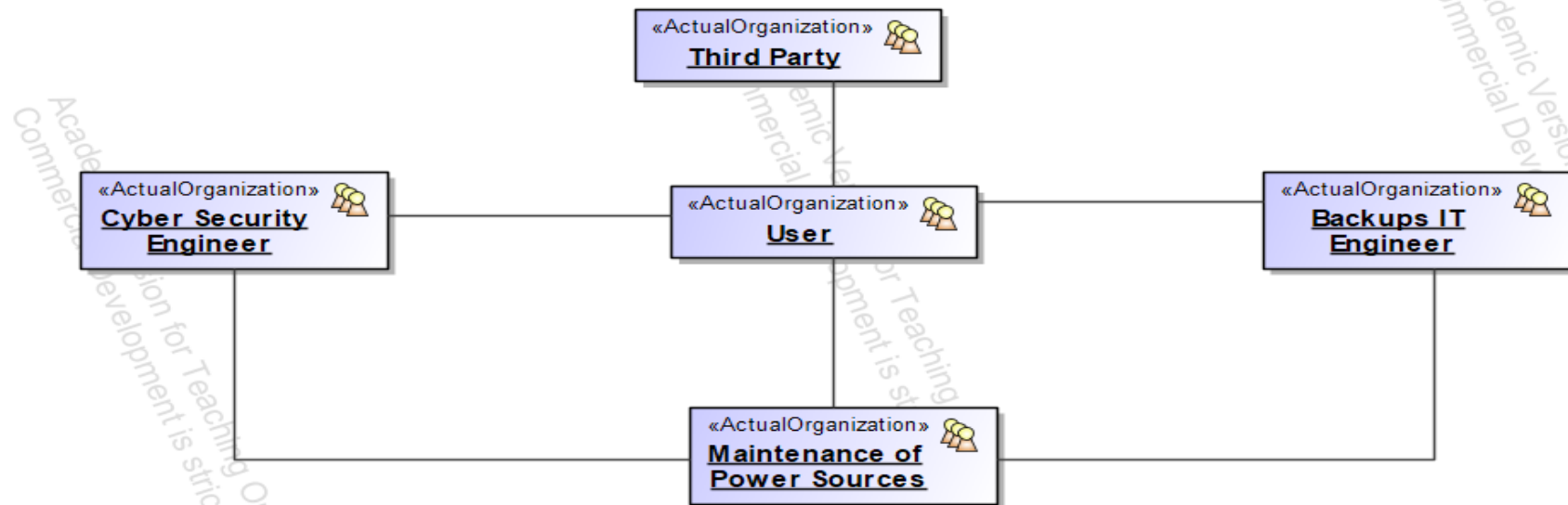
OV-2

OV-2 Operational Resource Flow Description [ OV-2]

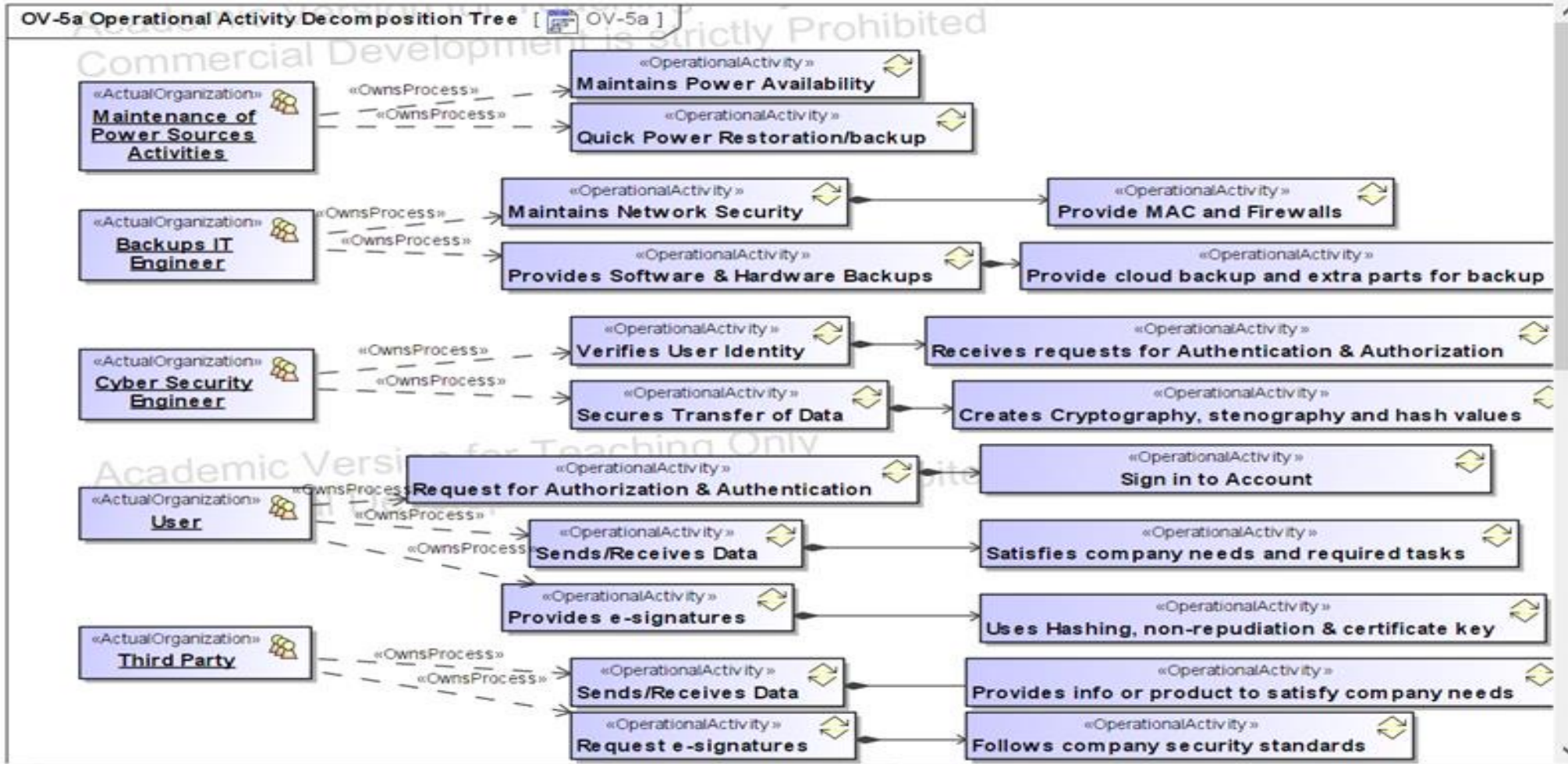


OV-4


OV-4 Organizational Relationships Chart [ OV-4]

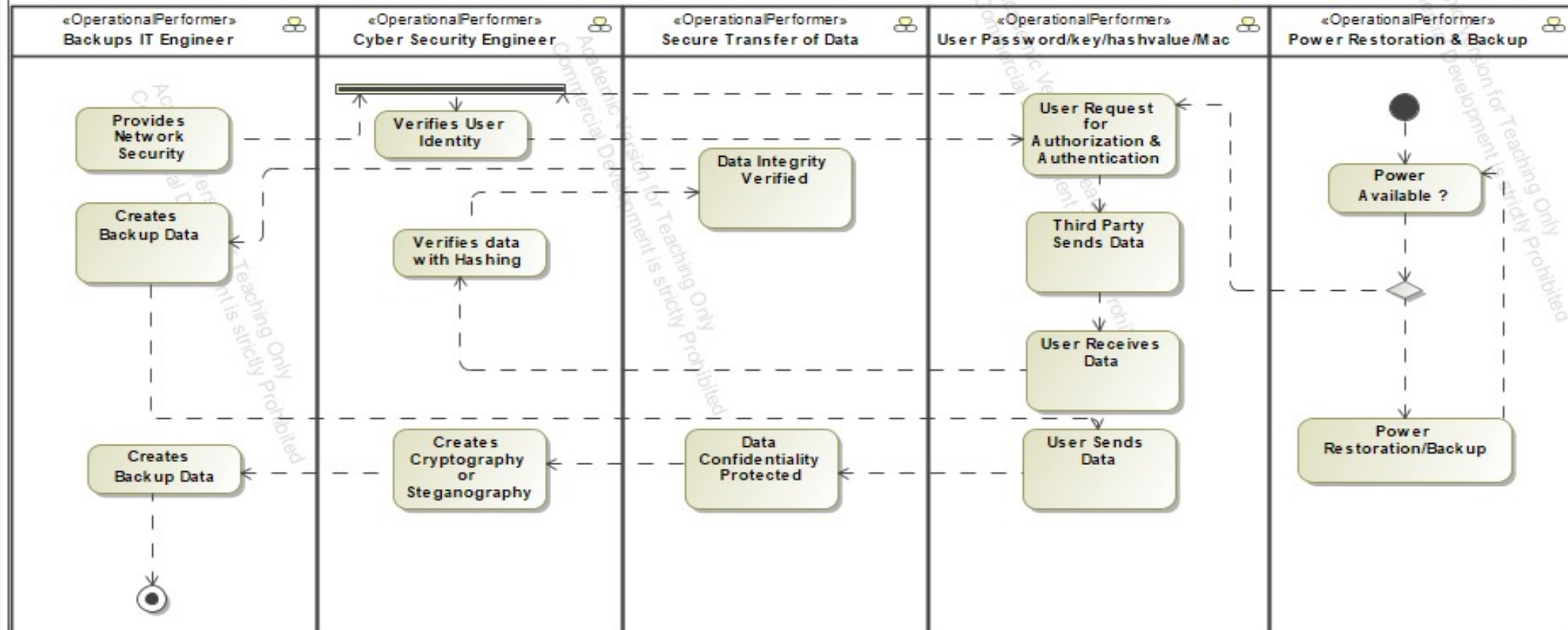


OV-5A



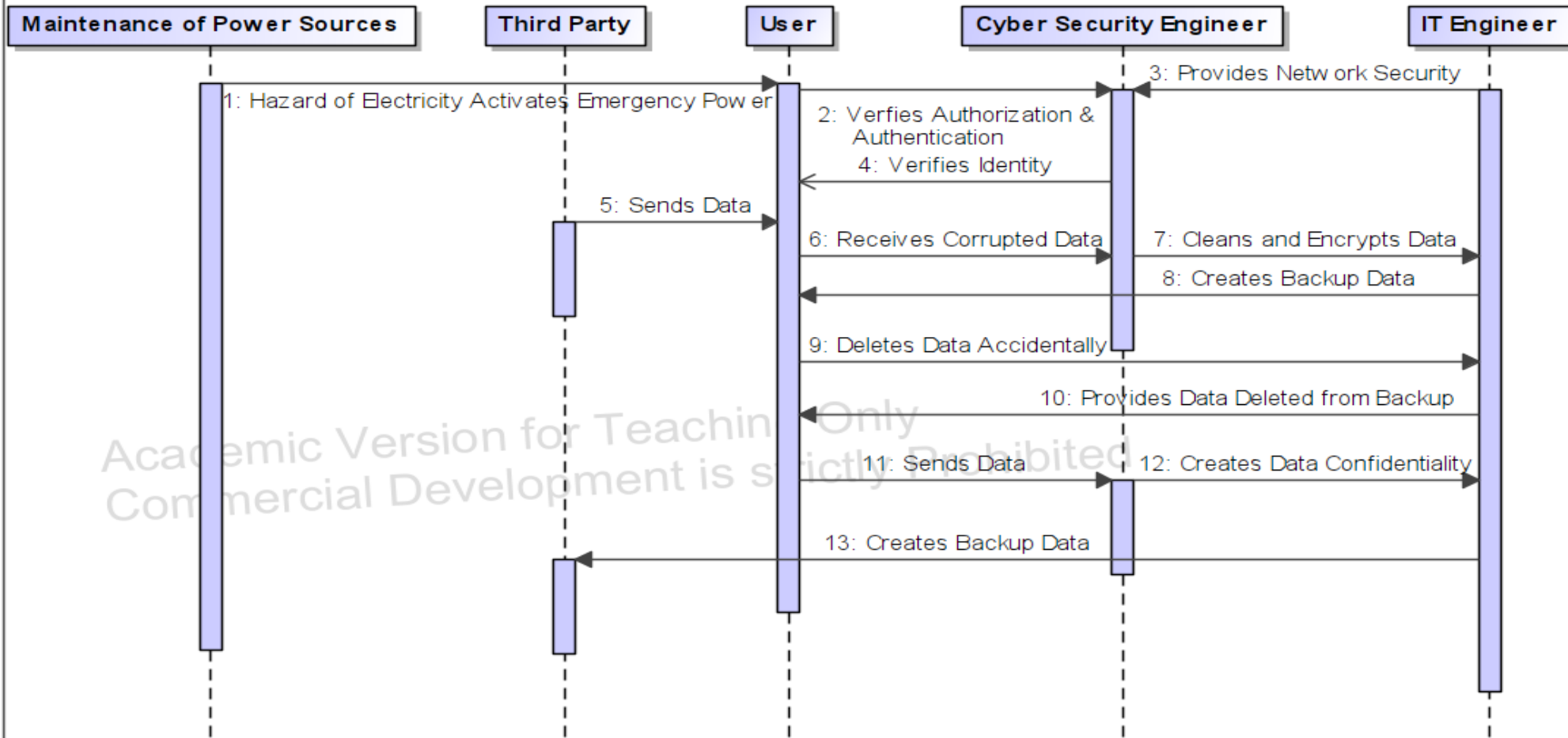
OV-5B

OV-5b Operational Activity Model [ OV-5b]

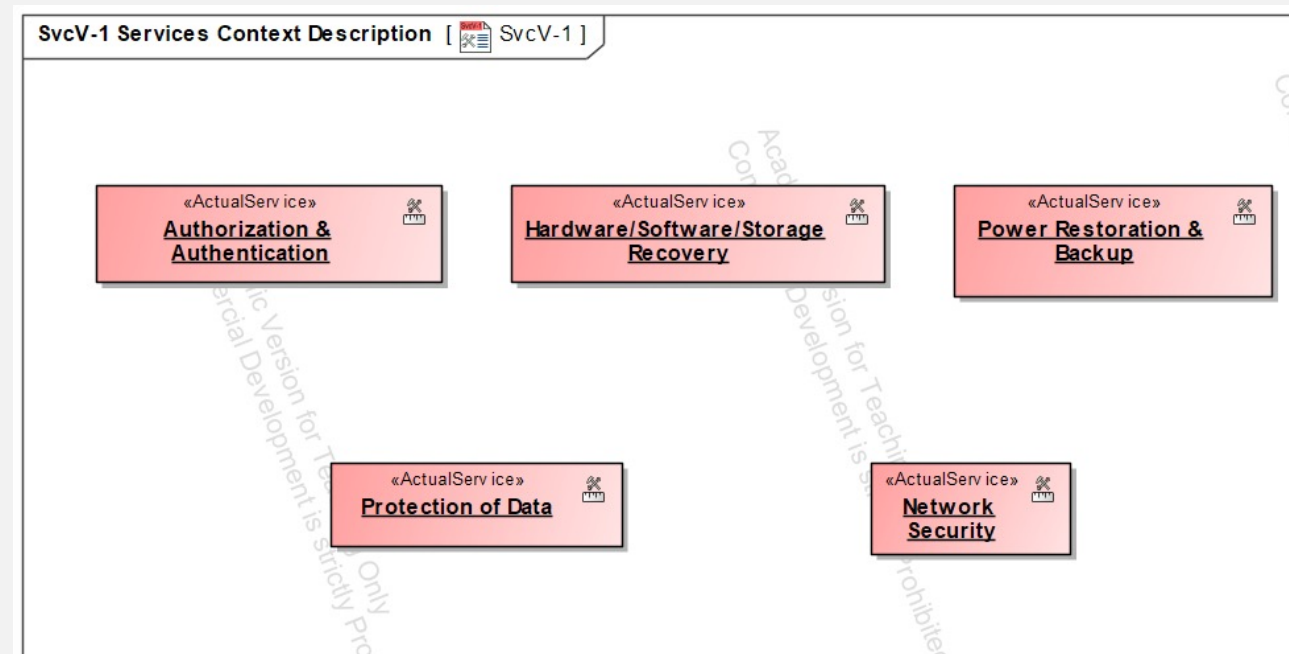


OV-6C

OV-6c Operational Event-Trace Description [OV-6c]

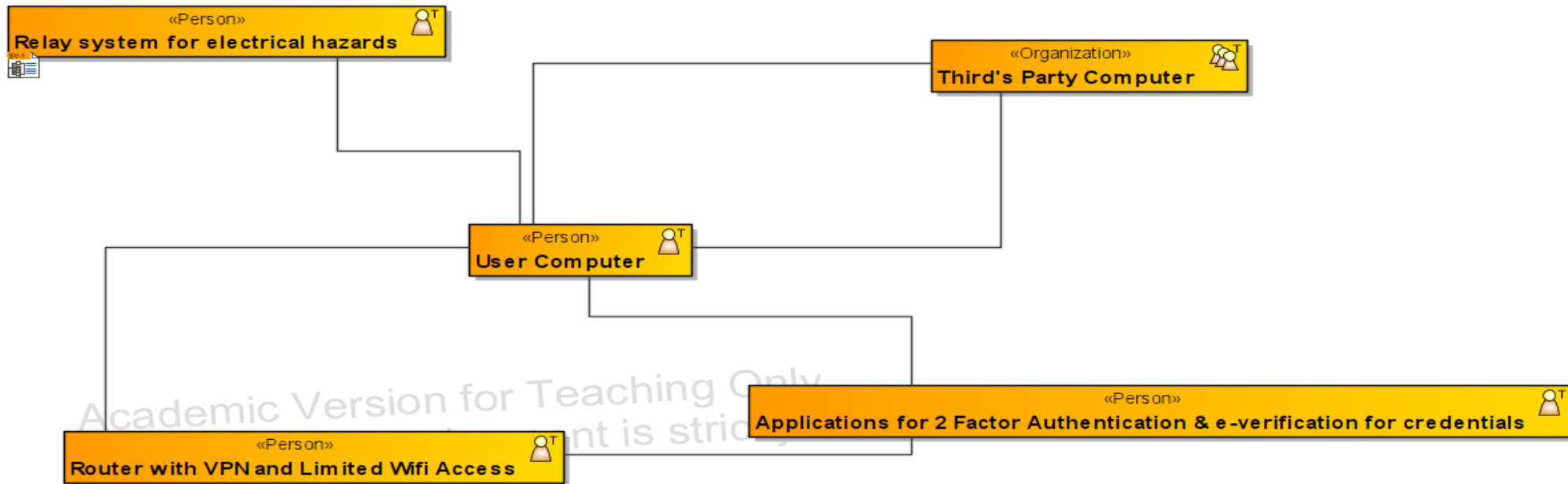


SVC-I SERVICES FUNCTIONALITY DESCRIPTION



SV-I SERVICES DIAGRAM

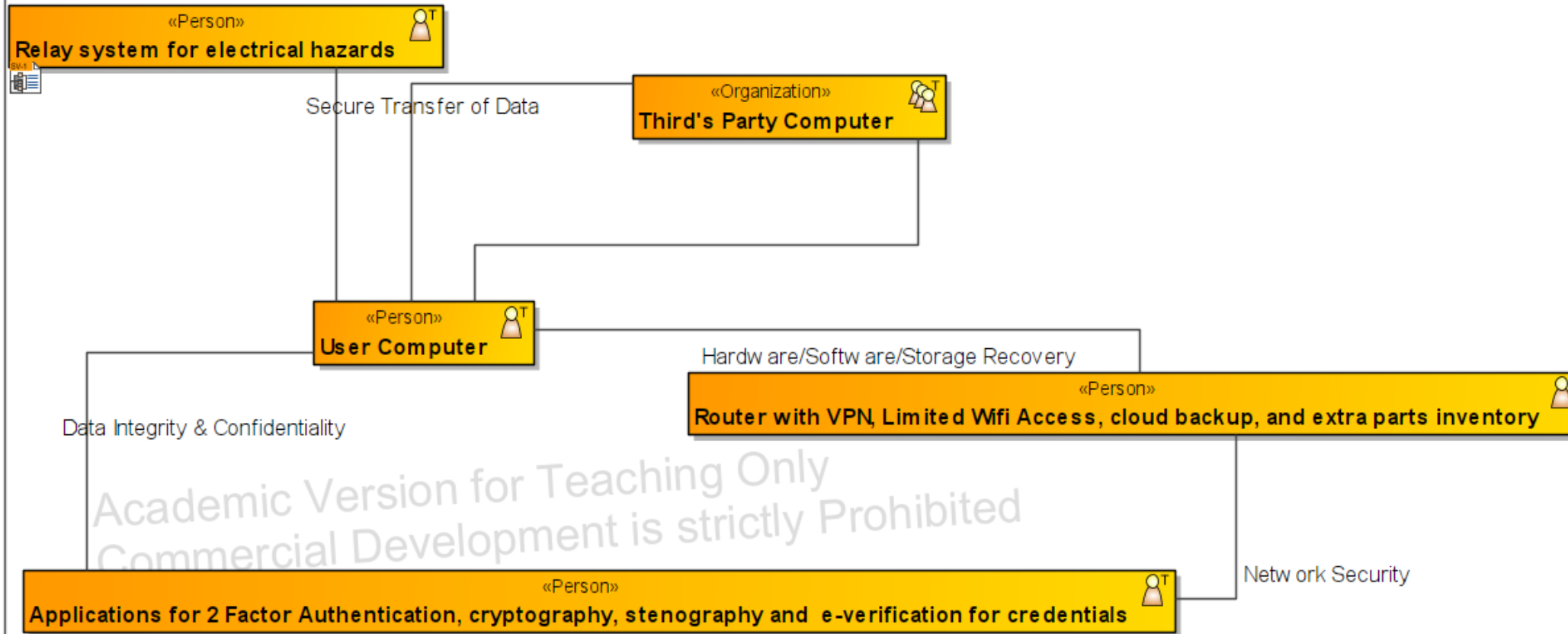
SV-1 Systems Interface Description [SV-1]



SV-2

SV-2 Systems Resource Flow Description [SV-2]

Power Restoration & Backup



MASTER LIST

MASTER LIST			
Super-type	Type	name	Definition
—	SuperCapability	Capabilities	—
—	Capability	Identifiability	—
—	Capability	Protectability	—
—	Capability	Detectability	—
—	Capability	Respond	—
—	Capability	Recoverability	—
—	Sub-Capability	Asset Management	—
—	Sub-Capability	Business Enviroment	—
—	Sub-Capability	Governance	—
—	Sub-Capability	Risk Assesment	—
—	Sub-Capability	Risk Management Strategy	—
—	Sub-Capability	Access Control	—
—	Sub-Capability	Awareness & Training	—
—	Sub-Capability	Data Security	—
—	Sub-Capability	IPPP	Information protection process & procedures
—	Sub-Capability	Maintenance	—
—	Sub-Capability	Protective Technology	—
—	Sub-Capability	Anomalies and Events	—
—	Sub-Capability	Continuous Monitoring	—
—	Sub-Capability	Detection Processes	—
—	Sub-Capability	Response Planning	—
—	Sub-Capability	Communications	—
—	Sub-Capability	Analysis	—
—	Sub-Capability	Mitigation	—
—	Sub-Capability	Improvements	—
—	Sub-Capability	Recovery Planning	—
—	Sub-Capability	Recovery Improvements	—
—	Sub-Capability	Recovery Communications	—
—	Vision	vision1	Guide Enterprises to obtain a balanced and secure enterprise security architecture to defend against cybersecurity threats ensuring alligment will support business needs
—	Goal	goal1	Build employees security culture, Generate a robust architecting for security, maintain continous improvement after recovery,redce silos, and govern process
—	OpActivity	Info Asset	—
—	OpActivity	Crypto Security	—
—	OpActivity	App software security	—
—	OpActivity	hardware security	—
—	OpActivity	Physical security	—
—	Services	Confidentiality	—
—	Services	Identification	—
—	Services	Registration	—
—	Services	Certification	—
—	Services	Directories	—
—	Services	Authentication	—
—	Services	Authorisation	—
—	Services	Access Control	—
—	Services	Audit Trail	—
Relation	Relation	relation1	—

RISK MATRIX



	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business Goals & Decisions	Business risk	Business Meta-process	Business Governance	Business geography	Business time dependencies

Risk management

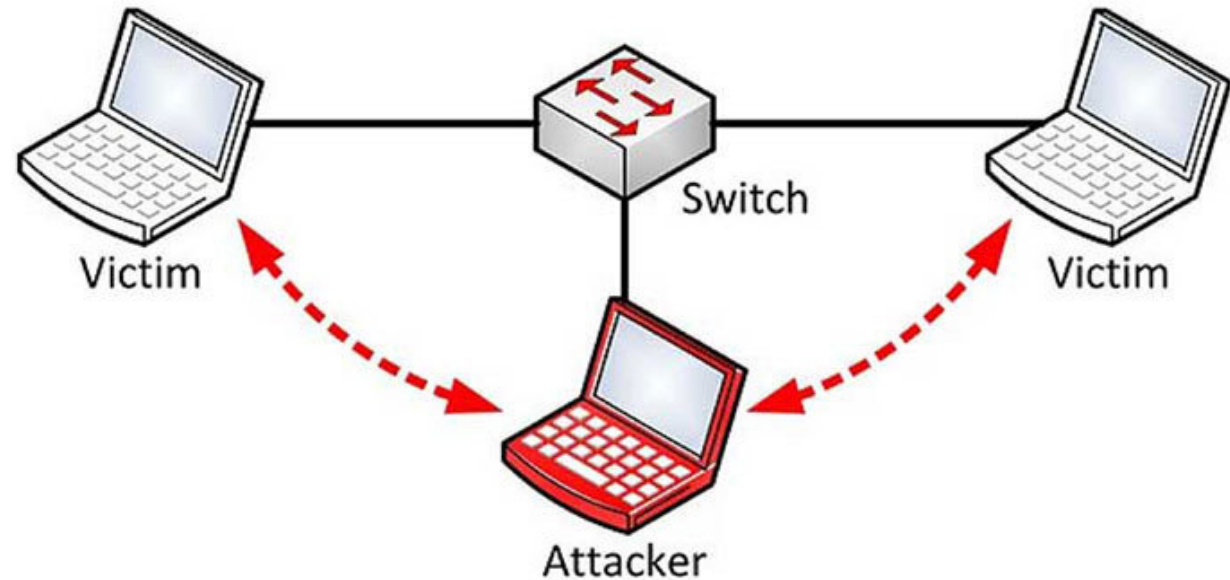
- 1. Identify the threats
- 2. Assess the vulnerability of critical assets to specific threats
- 3. Determine the risk (i.e. the expected likelihood and consequences of specific types of attacks on specific assets)
- 4. Identify ways to reduce those risks
- 5. Prioritize risk reduction measures

ISO 31000
ISO/IEC 27005
NIST Special Publication 800-37

LIKELIHOOD		I	M	P	A	C	T
		Negligible	Marginal		Critical		Catastrophic
	Certain	High	High		Extreme		Extreme
	Likely	Moderate	High		High		Extreme
	Possible	Low	Moderate		High		Extreme
	Unlikely	Low	Low		Moderate		Extreme
	Rare	Low	Low		Moderate		High

ATTACKERS

1. Malware
2. Phishing
3. Man-in-the-Middle Attacks
4. Denial-of-Service Attack
5. Password Attack





Cybersecurity tackles many aspects with focus on Integrity, Confidentiality, and Availability



Cybersecurity of a system is created in the inception with requirements and architecture.



There are many attack vectors to breach the system.



Cybersecurity only tackles a defender vs attacker perspective.



Cybersecurity is implemented after the architecture is created to determine and create strong points.

LESSONS LEARNED

SOURCES

- <https://www.cpomagazine.com/cyber-security/top-5-enterprise-security-threats-and-how-to-avoid-them/>
- <https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-cia-triad>
- <https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/>
- <https://www.incose.org/systems-engineering>
- <https://www.nist.gov/cyberframework>
- <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- <https://www.gsa.gov/technology/technology-products-services/it-security/nist-cybersecurity-framework-csf>
- <https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity>