Concordia Workshop - CS Consultant
Learning Objectives – Economics and Business

Muriel Franco, Bruno Rodrigues, Burkhard Stiller
Communication Systems Group CSG
Department of Informatics IFI
University of Zurich UZH

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

Agenda

- Introduction and Basics
- New Approaches
  - SEConomy Framework
- Discussion and Conclusions
- Hands-on Exercise

Introduction and Basics

Introduction

- As businesses and governments go digital, they are exposed to increasing number of threats
  - ⇨Governance, risk assessment, security assessment, and operations management are critical for digital era
- Cybersecurity is no longer “just” a technology perspective
  - ⇨ Societal and economic impacts equally important

Technology Intelligence

WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled [Telegraph, 2018]

Cybersecurity Facts

Frequency of **DDoS attacks** increased more than 2.5 times between 2014 and 2017 [Kaspersky 2018]

DDoS attacks averaged between **$ 20,000 - $ 40,000 per hour** [Kaspersky 2018]

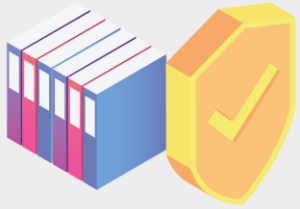
Cyber threats are increasing

Financial losses

34% of businesses hit with **Ransomware** took a week or more to regain access to their data [Symantec 2018]

The global Ransomware damage costs are **totaling around $ 11.5 billion** [Cybersecurity Ventures 2019]

CYBER SECURITY



Education, Prevention

Monitoring, Maintenance

Remediation, Insurance

Cybersecurity Economics' Basics

- Many problems plaguing cybersecurity are economic in nature
  - Systems fail because the organizations often fail to assess the risks of failure
  - Regulatory interventions may be necessary to strengthen cybersecurity measures, hardening, or awareness (the least)
    - *E.g.*, based on ENISA, ISO, and NIST
- Different costs have to be considered during the planning on cybersecurity support measures

$$\underbrace{Risks}_{\substack{\text{financial loss} \\ \text{reputation loss}}} \rightarrow CAPEX + OPEX$$

CAPEX: Capital Expenditures, OPEX: Operational Expenditures

New Approaches

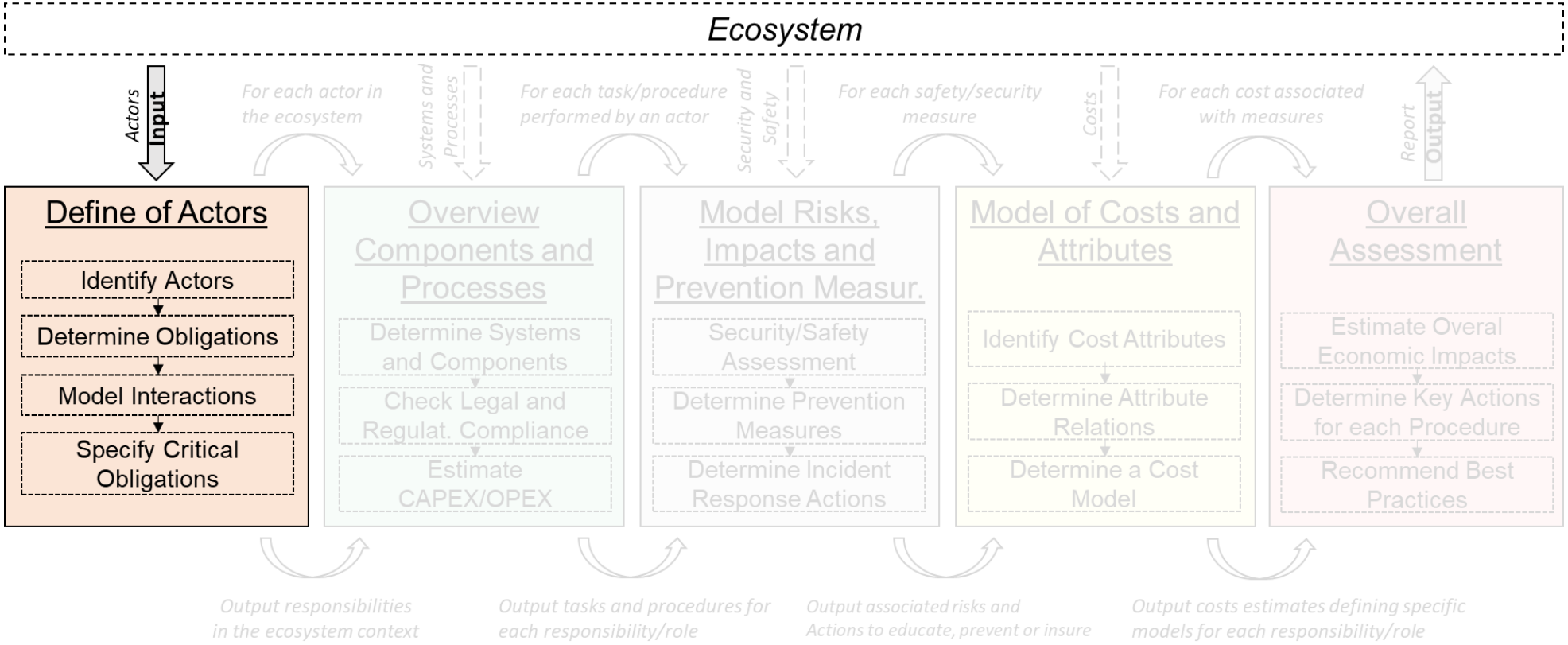
SEConomy Framework

SEConomy Framework Overview

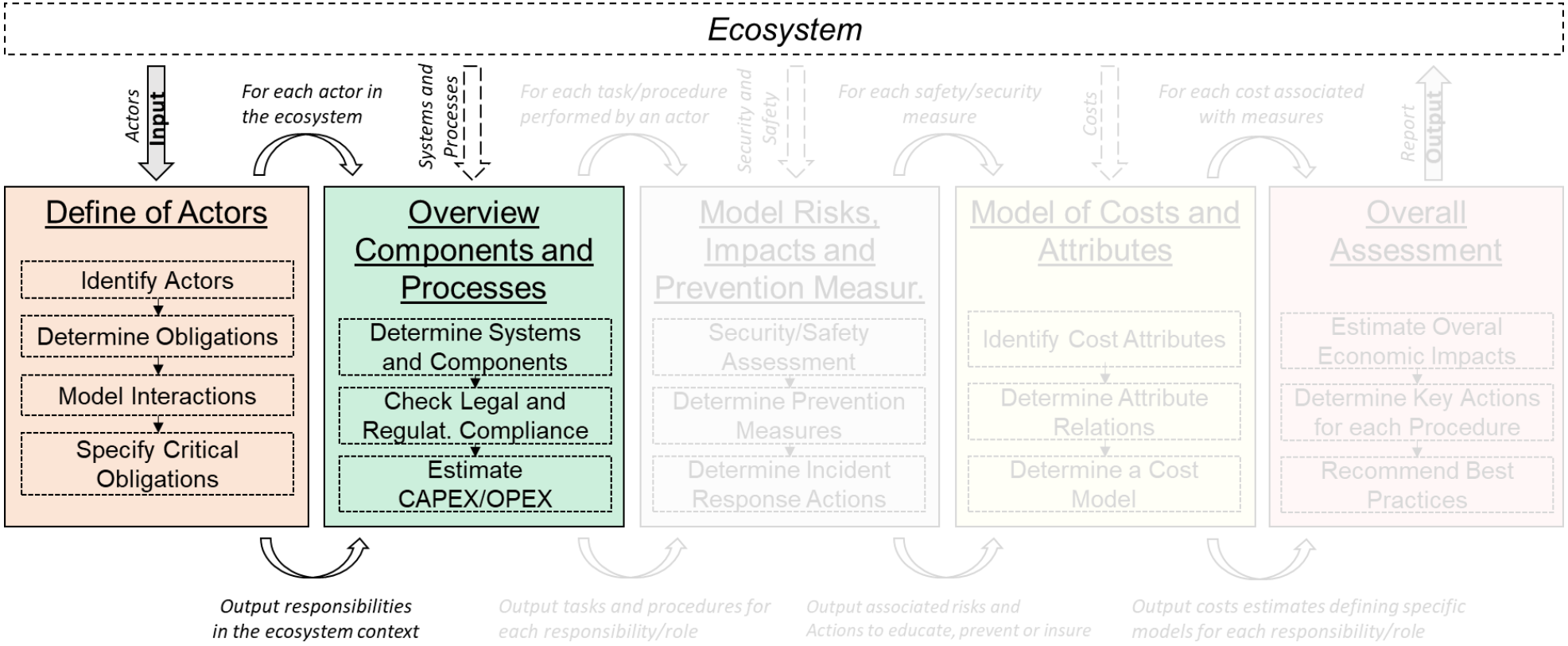
- Identify security risks and associated costs
  - Mapping/modelling specific attributes and their relation
- Determine impacts of cyber (in)security in the economy
  - Education, prevention, remediation, insurance

- SEConomy is a framework to assess cybersecurity economics
  - Structured view on critical actors, roles and processes, and their associated critical tasks
  - Map of risk-dependencies between systems and related systems/subsystems
  - Associate time-dynamics with classes of costs

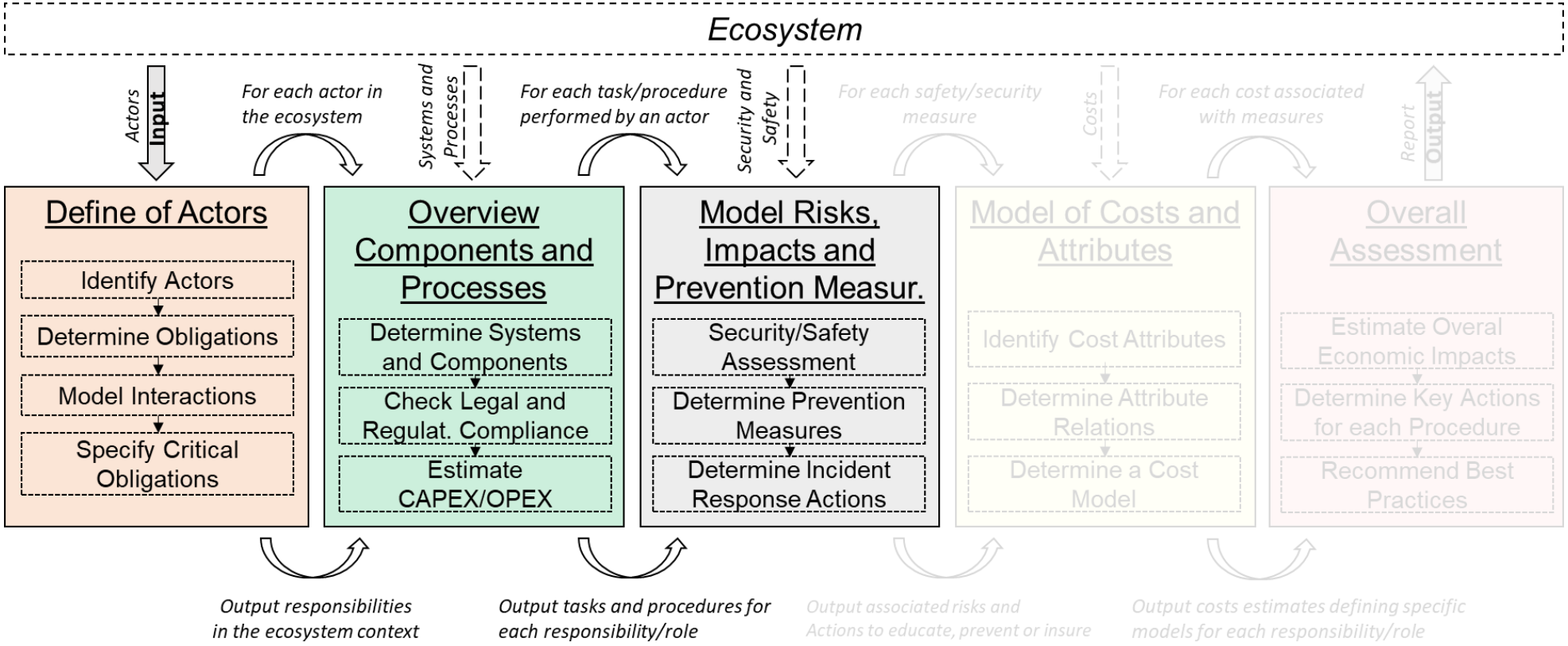
Step-based Approach



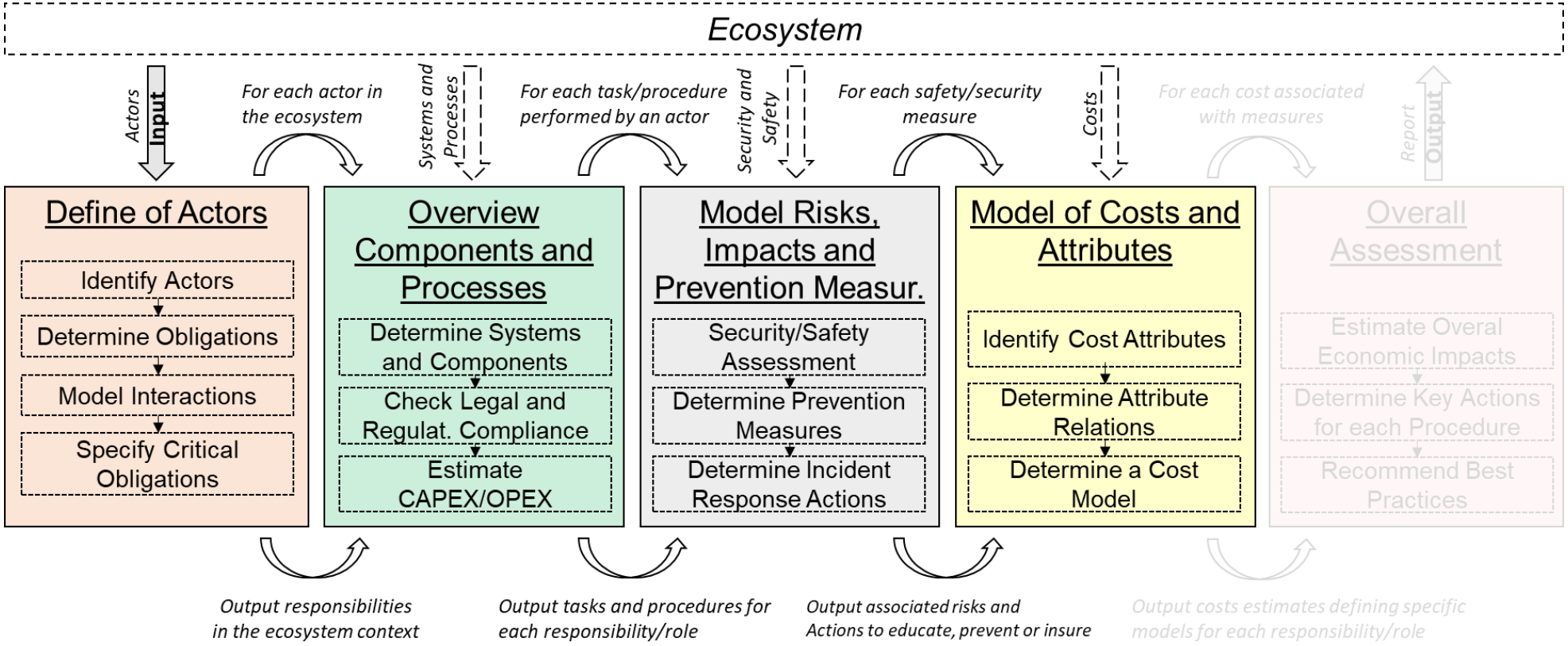
Step-based Approach



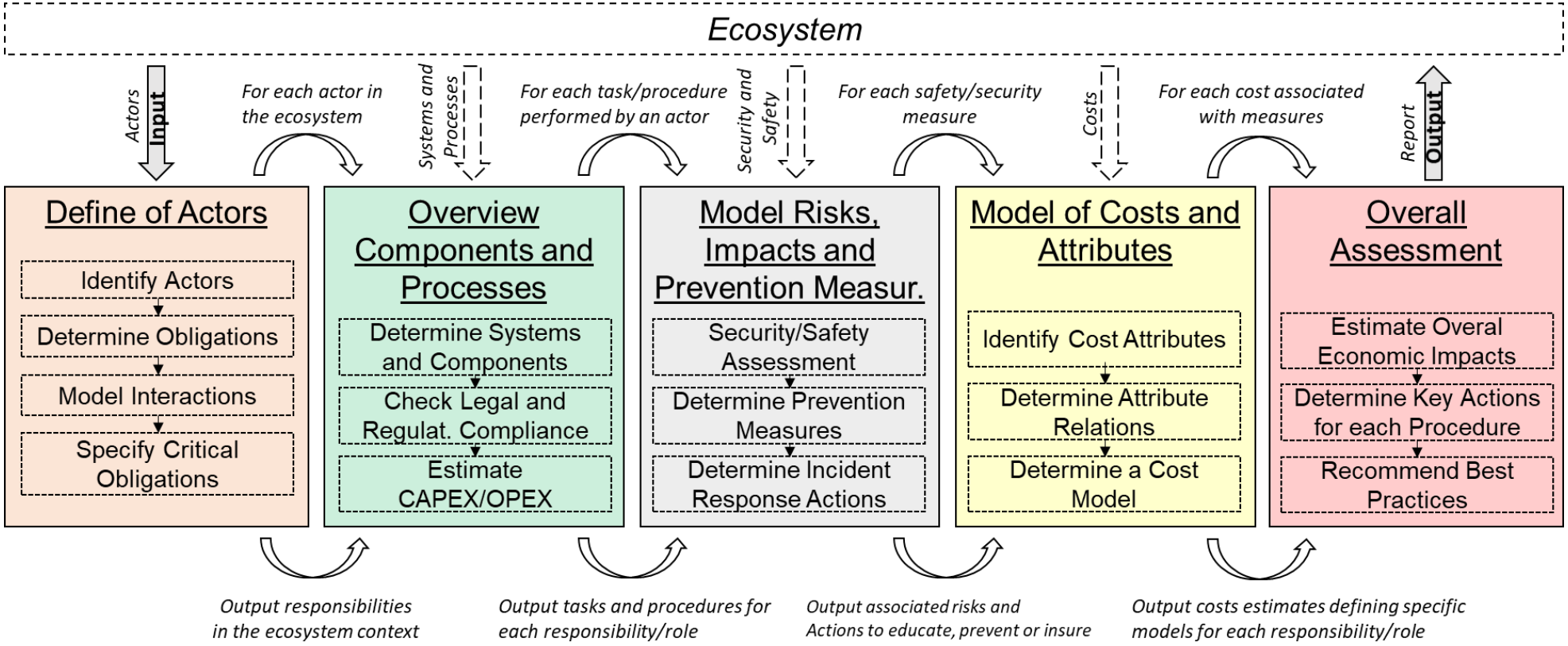
Step-based Approach



Step-based Approach



Step-based Approach



Overall Cost Assessment

Algorithm 1: Overall Economic Assessment (OEA)

```
1  begin
2      for each Actor ∈ Ecosystem:
3          for each Role ∈ Actor:
4              for each System ∈ Role:
                   /* Correlation between linked systems in Equation 1  */
5                  p(x) ← dependence(System, ∀ linkedSystems)
                   /* Estimate exposure costs in Equation 2             */
6                  threat_costs ← T_costs(A, p(x))
                   /* Estimate mitigation (Proactive and Reactive) costs
                      in Equation 3                                     */
7                  mitigation_costs ← PMCcosts(A)
8                  mitigation_costs ← RMCcosts(A, p(x))
                   /* Get Overal Economic Assessment (OEA) in Equation 4
                      */
9                  OEA ← ROSI(threat_costs, mitigation_costs, InitSecCost)
```

$$ROSI = \Delta T * \sum_{i=1}^{N_{System}} \frac{(T_{costs} * RMC) - PMC}{PMC}$$

Discussion and Conclusions

Conclusions

- Cybersecurity economics involves a broad of activities
  - Education, prevention, monitoring, maintenance, remediation, insurance
- It is critical to map systems and processes and their correlations as well as related costs
  - Novel frameworks, standardizations, and techniques
  - Training and education focusing on the demands and threats of the different sectors
- Approaches that help during the decision process and planning of cybersecurity are crucial for stakeholders
  - e.g., Customers, companies, and cyber insurers

Hands-on Exercise

Hands-on Exercise

- CONCORDIA internally selected Knowledge and Skills linked to LO3 (Economics and Business)
- Top-20 Knowledge
- Top-10 Skills

- Which LO3 Knowledge and Skills are important for your industry sector?

https://concordia.monitorboard.nl

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

™

www.linkedin.com/in/concordia-h2020