UNIVERSITY OF SOUTH BRITTANY

FACULTY OF SCIENCES AND ENGINEERING

MASTER 1 CYBERUS

PROJECT

NIST Risk Management Standards

Created by:

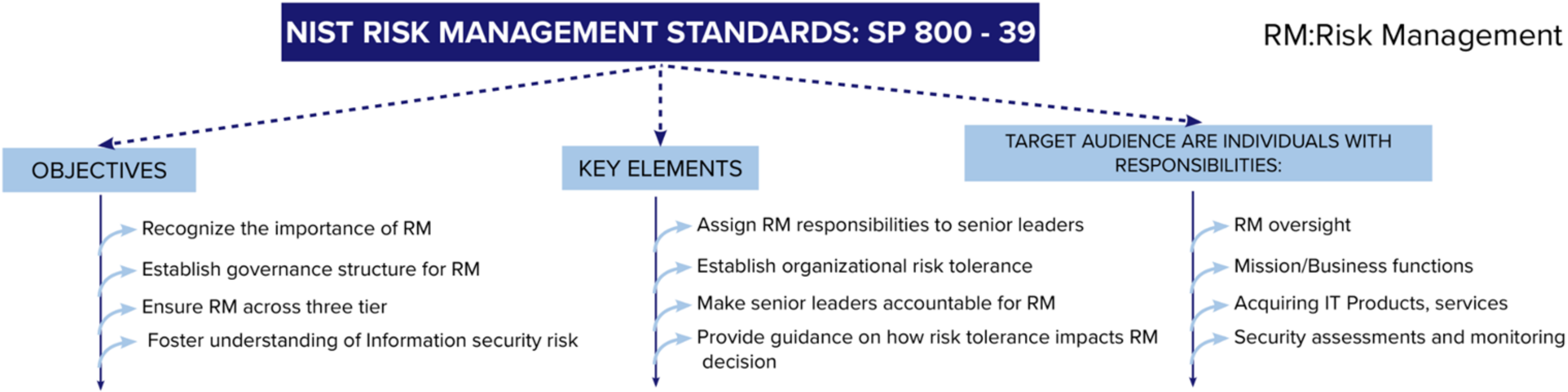
Amarilda Koka
Dang Kien Nguyen
Fatih Durmaz
Ibrahim Yaghi
Paweł Borsukiewicz

Ribiea Ramzan
Renée Duhaney
Tosin Osunwale
Yousra Taryous
Zakaria Belkadi

Led by:
Stéphane PAUL

INTRODUCTION

RM:Risk Management



NIST RISK MANAGEMENT STANDARDS: SP 800 - 39

OBJECTIVES

- Recognize the importance of RM
- Establish governance structure for RM
- Ensure RM across three tier
- Foster understanding of Information security risk

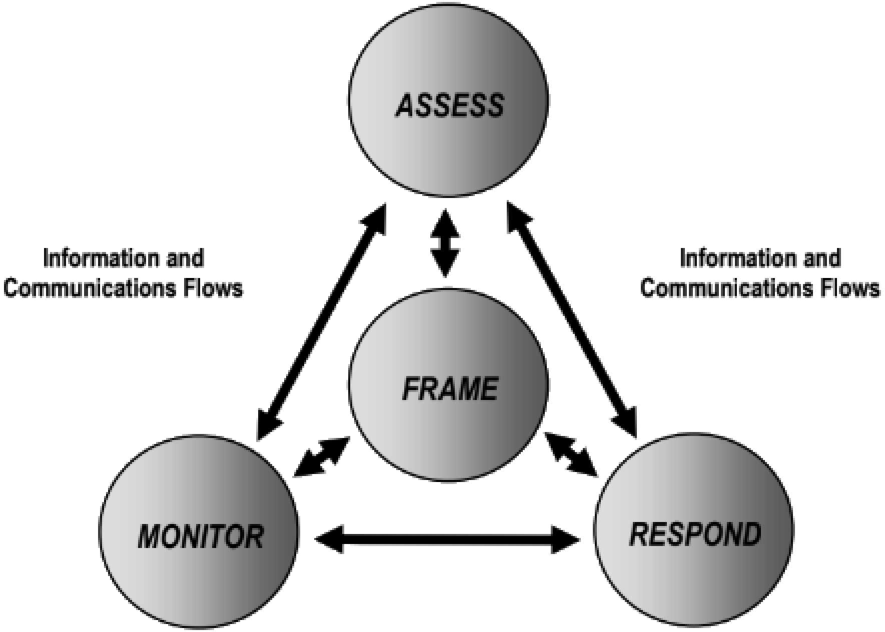
KEY ELEMENTS

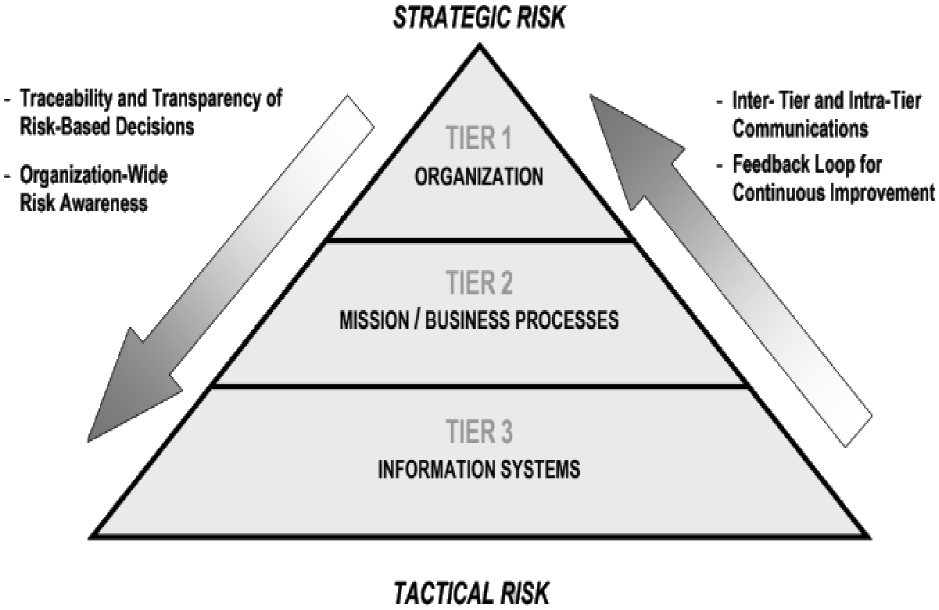
- Assign RM responsibilities to senior leaders
- Establish organizational risk tolerance
- Make senior leaders accountable for RM
- Provide guidance on how risk tolerance impacts RM decision

TARGET AUDIENCE ARE INDIVIDUALS WITH RESPONSIBILITIES:

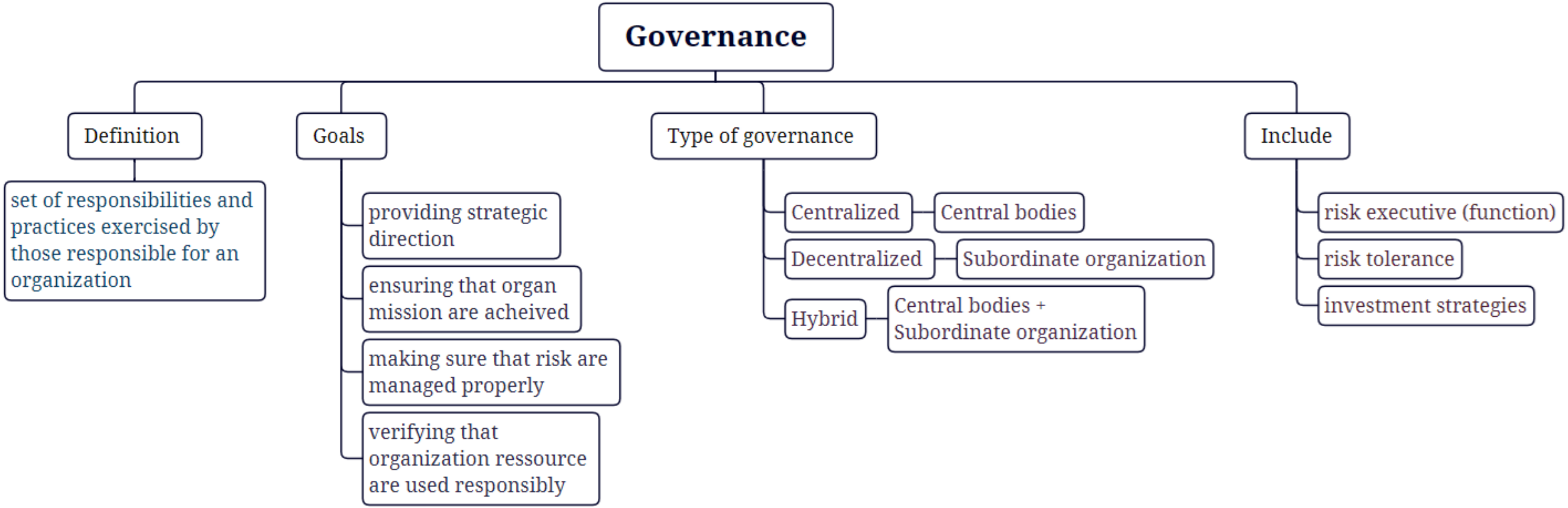
- RM oversight
- Mission/Business functions
- Acquiring IT Products, services
- Security assessments and monitoring

THE FUNDAMENTALS

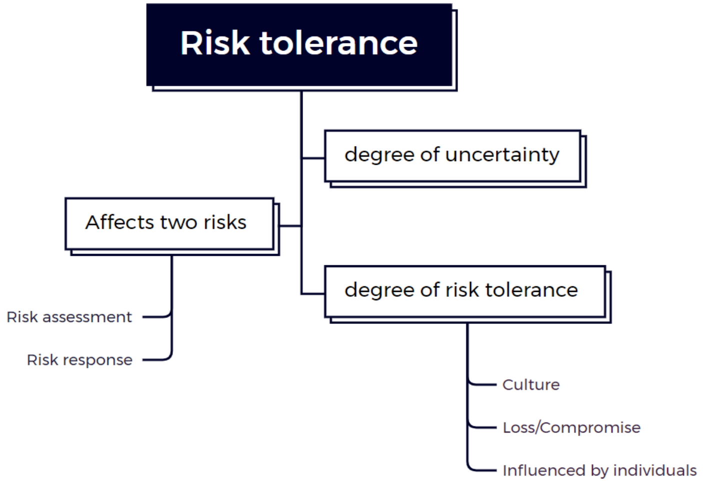

ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

Tier One - Organization view

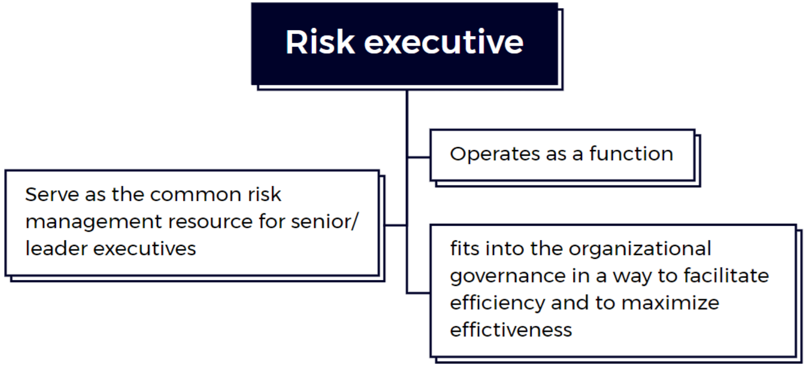


- **Governance**
  - Definition
    - set of responsibilities and practices exercised by those responsible for an organization
  - Goals
    - providing strategic direction
    - ensuring that organ mission are acheived
    - making sure that risk are managed properly
    - verifying that organization ressource are used responsibly
  - Type of governance
    - Centralized — Central bodies
    - Decentralized — Subordinate organization
    - Hybrid — Central bodies + Subordinate organization
  - Include
    - risk executive (function)
    - risk tolerance
    - investment strategies



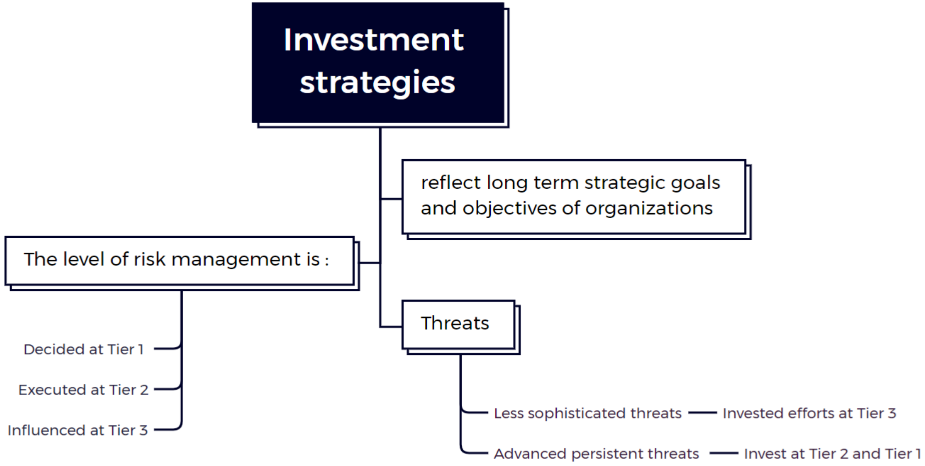
Risk tolerance

- degree of uncertainty
- Affects two risks
  - Risk assessment
  - Risk response
- degree of risk tolerance
  - Culture
  - Loss/Compromise
  - Influenced by individuals



Risk executive

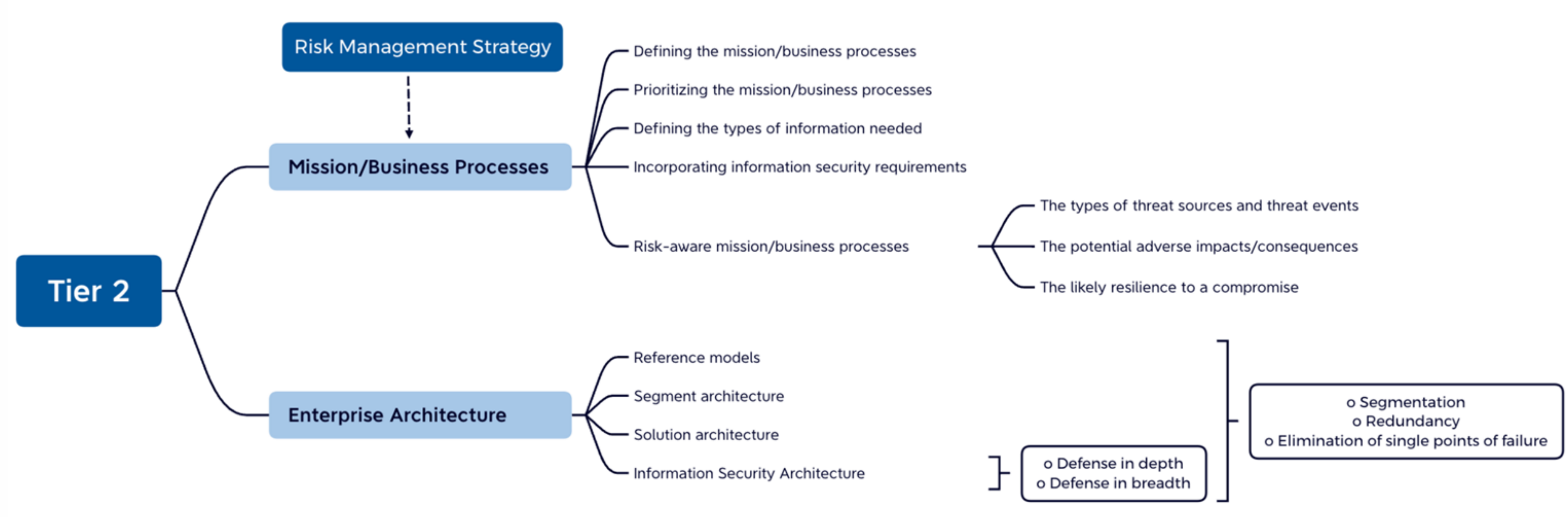
- Operates as a function
- Serve as the common risk management resource for senior/ leader executives
- fits into the organizational governance in a way to facilitate efficiency and to maximize effictiveness



Investment strategies

- reflect long term strategic goals and objectives of organizations
- The level of risk management is :
  - Decided at Tier 1
  - Executed at Tier 2
  - Influenced at Tier 3
- Threats
  - Less sophisticated threats — Invested efforts at Tier 3
  - Advanced persistent threats — Invest at Tier 2 and Tier 1

Tier Two - Mission/Business Process View



Risk Management Strategy

Tier 2

- Mission/Business Processes
  - Defining the mission/business processes
  - Prioritizing the mission/business processes
  - Defining the types of information needed
  - Incorporating information security requirements
  - Risk-aware mission/business processes
    - The types of threat sources and threat events
    - The potential adverse impacts/consequences
    - The likely resilience to a compromise
- Enterprise Architecture
  - Reference models
  - Segment architecture
  - Solution architecture
  - Information Security Architecture
    - o Defense in depth
    - o Defense in breadth
      - o Segmentation
      - o Redundancy
      - o Elimination of single points of failure

Tier Three - Information Systems View

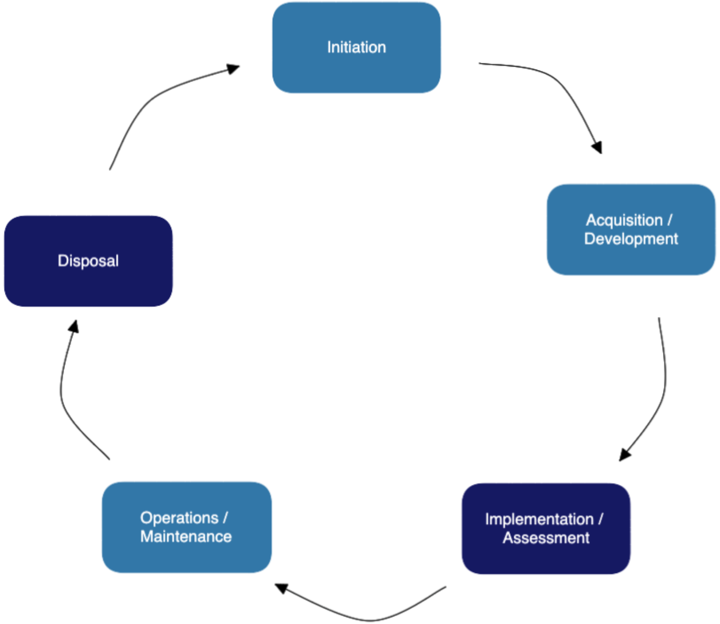
Initiation: Information security requirements are elicited based on threat information.

Acquisition/Development: Organisations mitigate potential design-related vulnerabilities.

Implementation: Selected security controls are monitored and assessed.

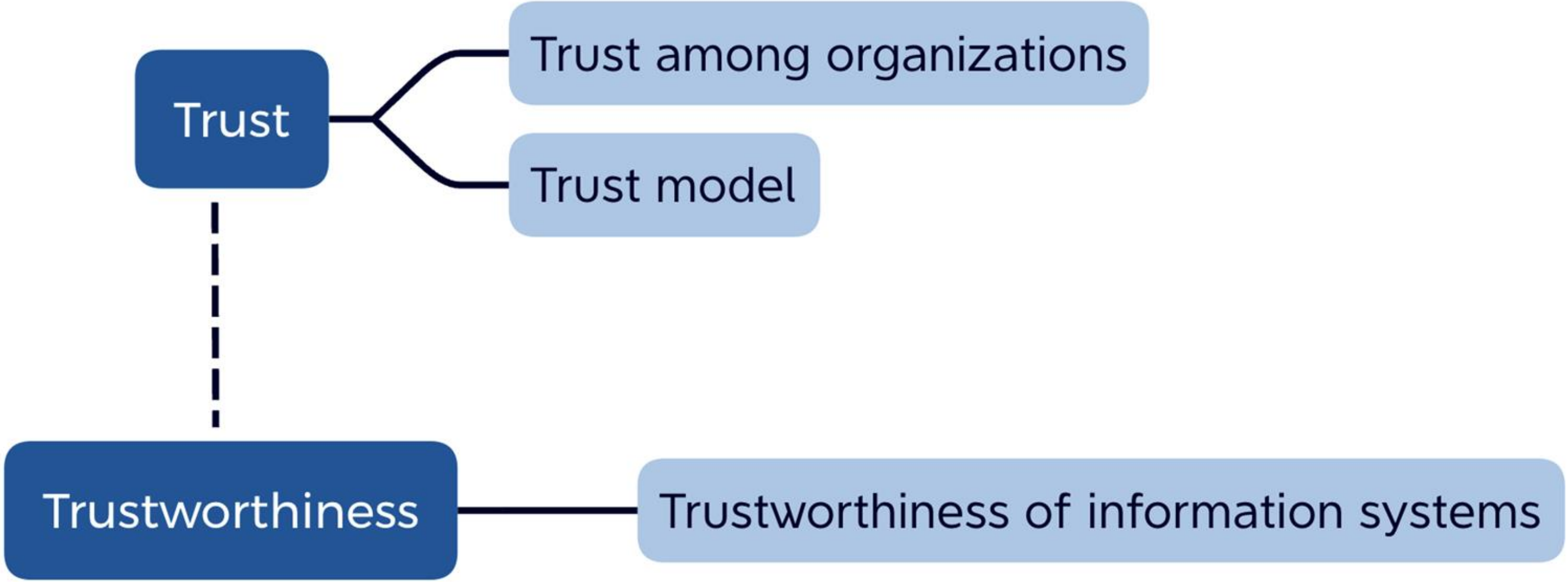
Operations: Security control effectiveness are monitored.

Disposal: Organisations remove any information that may cause adverse impacts, if compromised.



Systems Development Life Cycle

Trust and Trustworthiness



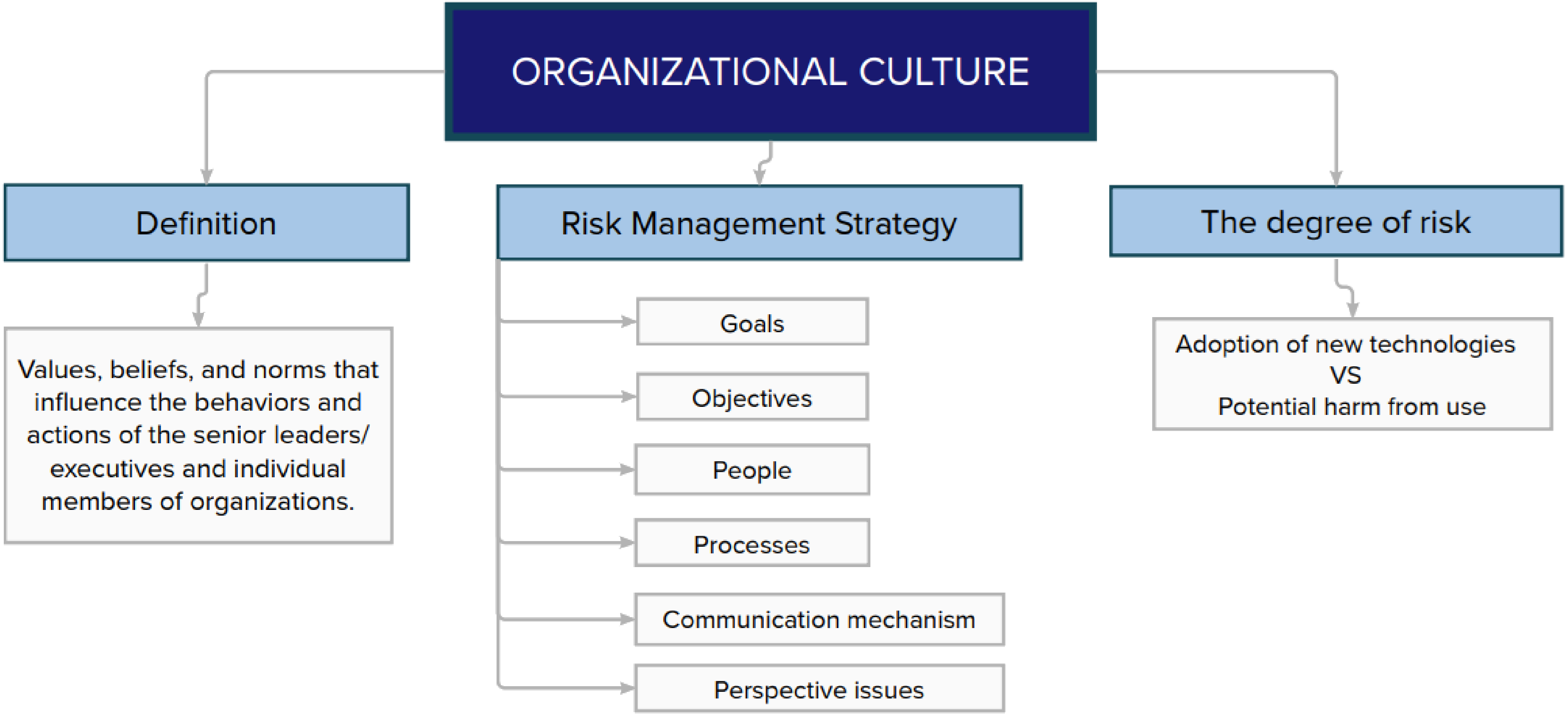
Trust

Trust among organizations

Trust model

Trustworthiness

Trustworthiness of information systems



ORGANIZATIONAL CULTURE

Definition

Values, beliefs, and norms that influence the behaviors and actions of the senior leaders/ executives and individual members of organizations.

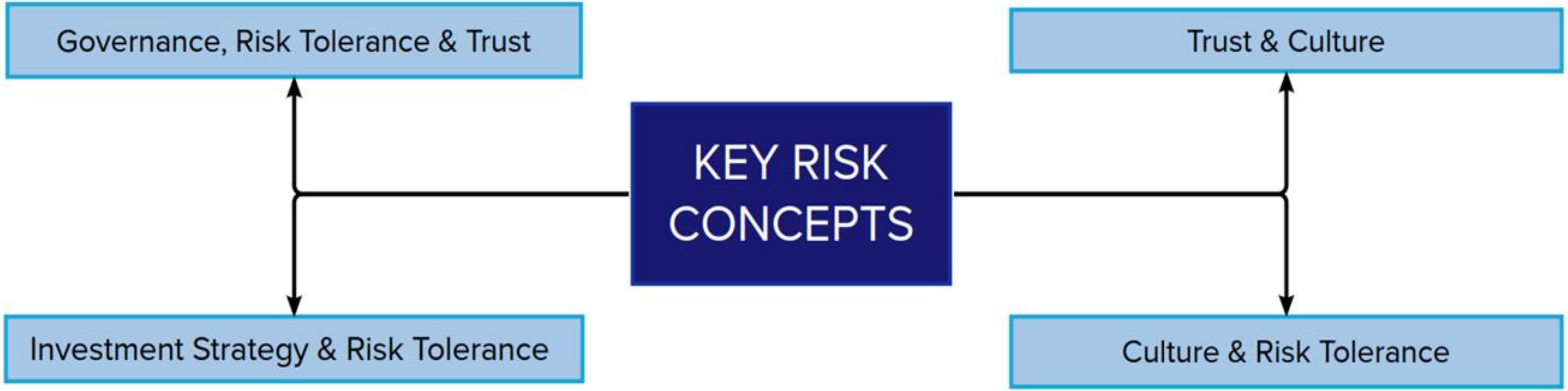
Risk Management Strategy

- Goals
- Objectives
- People
- Processes
- Communication mechanism
- Perspective issues

The degree of risk

Adoption of new technologies
VS
Potential harm from use

Relationship Among Key Risk Concepts



Governance, Risk Tolerance & Trust

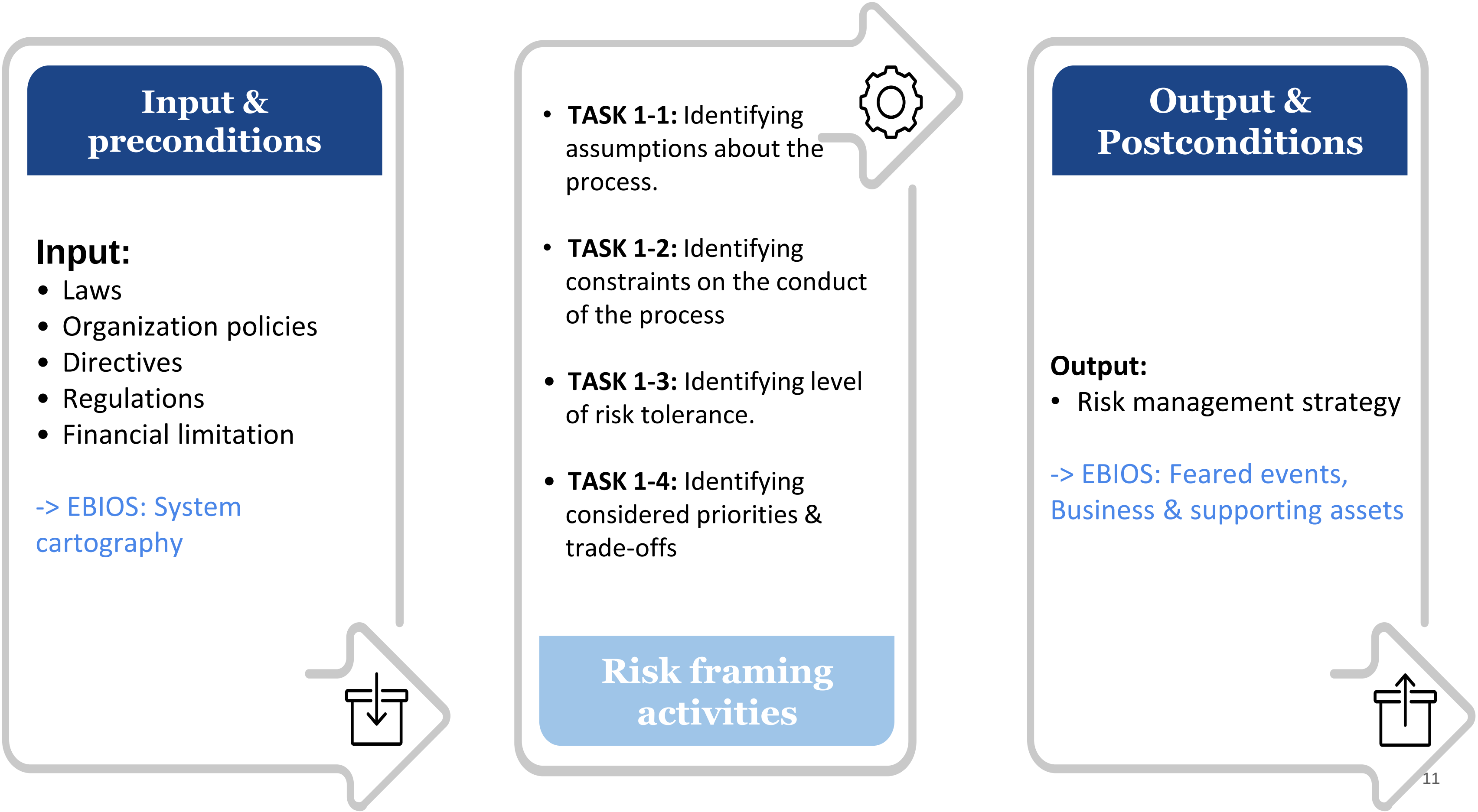
Trust & Culture

KEY RISK CONCEPTS

Investment Strategy & Risk Tolerance

Culture & Risk Tolerance

Risk Framing



Input & preconditions

Input:

- Laws
- Organization policies
- Directives
- Regulations
- Financial limitation

-> EBIOS: System cartography

- **TASK 1-1:** Identifying assumptions about the process.
- **TASK 1-2:** Identifying constraints on the conduct of the process
- **TASK 1-3:** Identifying level of risk tolerance.
- **TASK 1-4:** Identifying considered priorities & trade-offs

Risk framing activities

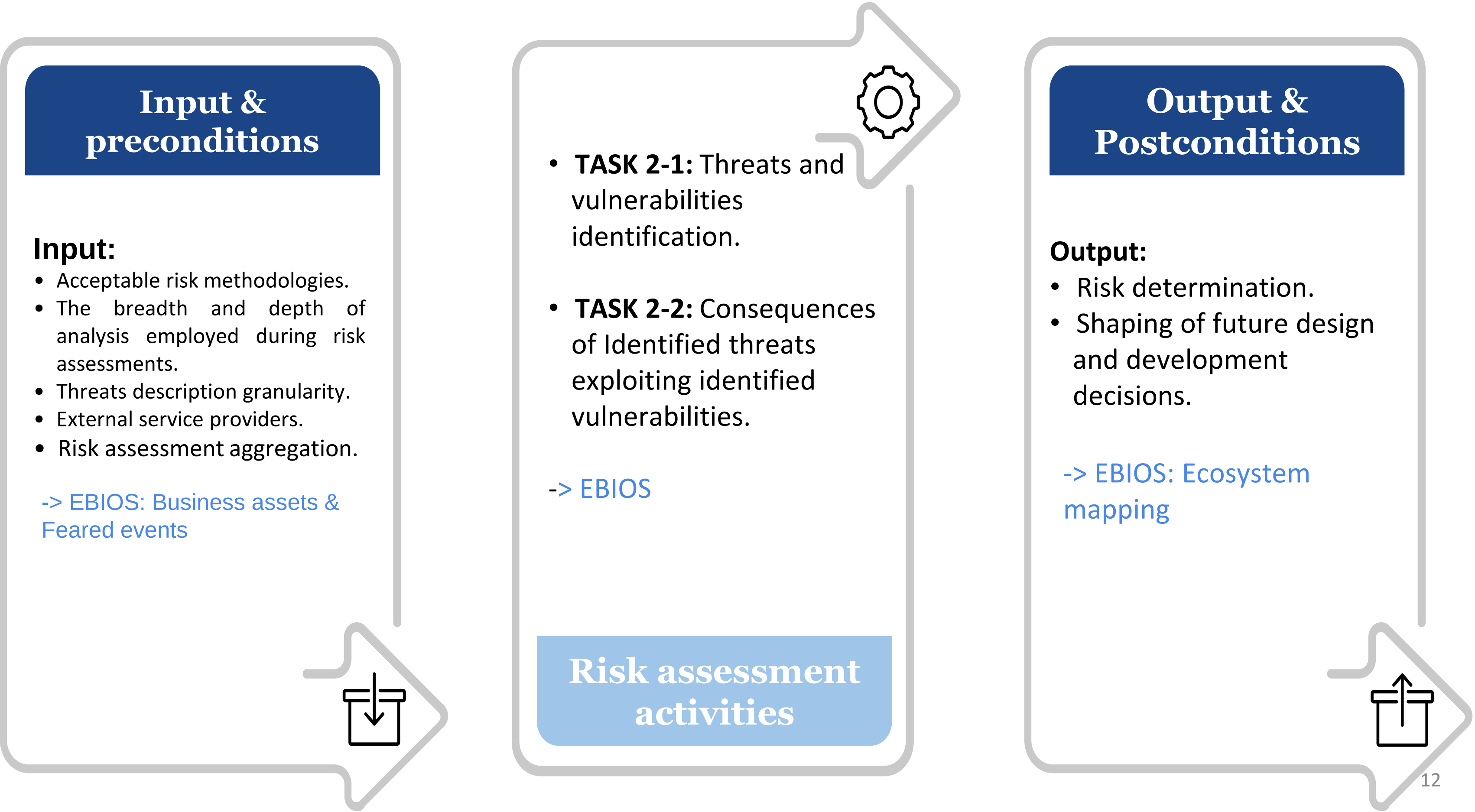
Output & Postconditions

Output:

- Risk management strategy

-> EBIOS: Feared events, Business & supporting assets

Risk Assessment Steps



Input & preconditions

Input:

- Acceptable risk methodologies.
- The breadth and depth of analysis employed during risk assessments.
- Threats description granularity.
- External service providers.
- Risk assessment aggregation.

-> EBIOS: Business assets & Feared events

Risk assessment activities

- **TASK 2-1:** Threats and vulnerabilities identification.
- **TASK 2-2:** Consequences of Identified threats exploiting identified vulnerabilities.

-> EBIOS

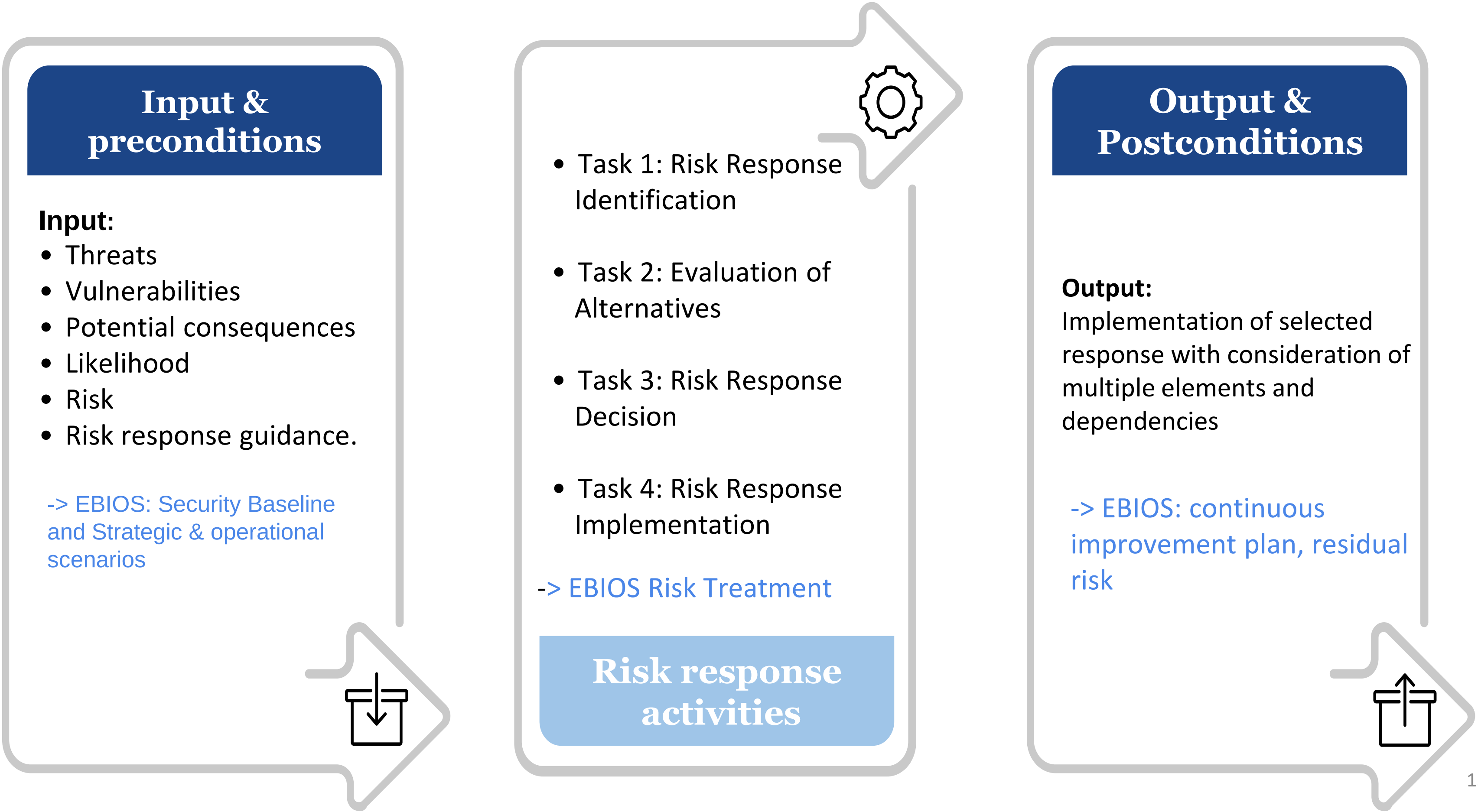
Output & Postconditions

Output:

- Risk determination.
- Shaping of future design and development decisions.

-> EBIOS: Ecosystem mapping

Risk Response Steps



Input & preconditions

Input:

- Threats
- Vulnerabilities
- Potential consequences
- Likelihood
- Risk
- Risk response guidance.

-> EBIOS: Security Baseline and Strategic & operational scenarios

- Task 1: Risk Response Identification
- Task 2: Evaluation of Alternatives
- Task 3: Risk Response Decision
- Task 4: Risk Response Implementation

-> EBIOS Risk Treatment

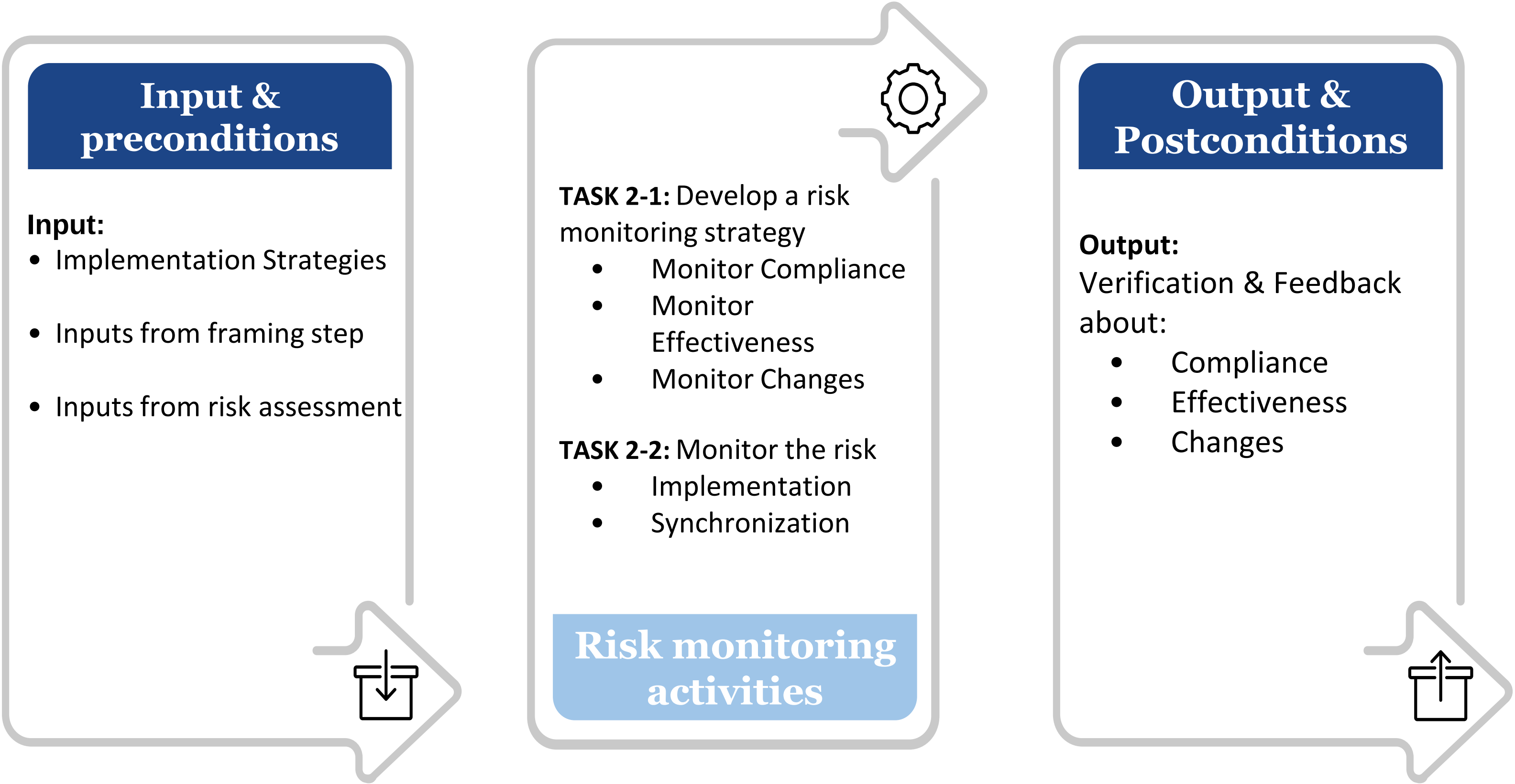
Risk response activities

Output & Postconditions

Output:
Implementation of selected response with consideration of multiple elements and dependencies

-> EBIOS: continuous improvement plan, residual risk

Risk Monitoring



Input & preconditions

Input:

- Implementation Strategies
- Inputs from framing step
- Inputs from risk assessment

TASK 2-1: Develop a risk monitoring strategy

- Monitor Compliance
- Monitor Effectiveness
- Monitor Changes

TASK 2-2: Monitor the risk

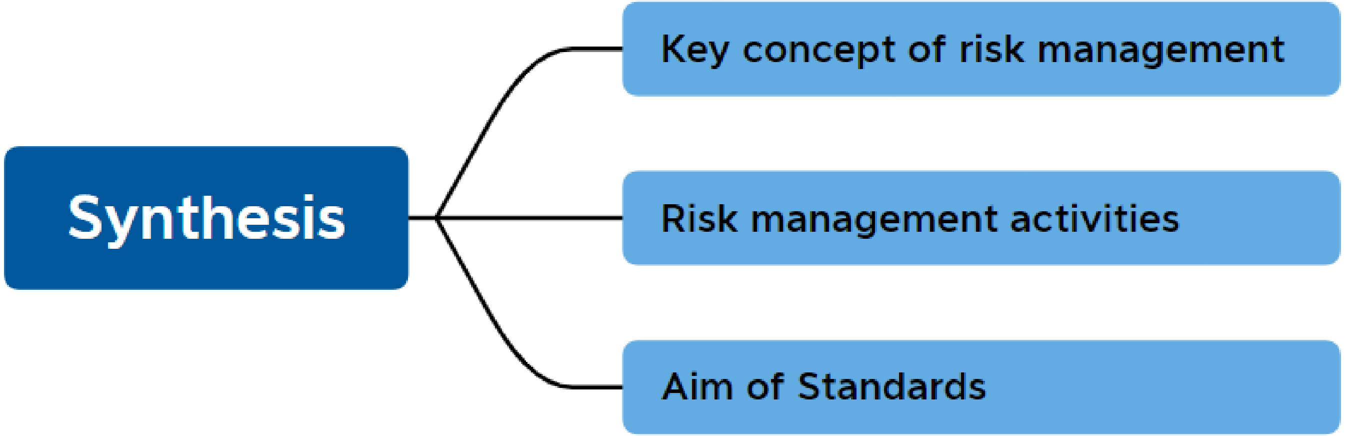
- Implementation
- Synchronization

Risk monitoring activities

Output & Postconditions

Output:
Verification & Feedback about:

- Compliance
- Effectiveness
- Changes



Synthesis

Key concept of risk management

Risk management activities

Aim of Standards