Assessing Risk and Cyber Resiliency

Is the accepted formula for risk (Risk = Vulnerability × Threat × Impact) usable when dealing with cyber resilience? For example, is there really any way to quantify the number of vulnerabilities in my entire network? If the answer to this question is "no", this then brings into question our ability to measure risk using the above formula.

This task asks the question: Is there a better way to measure risk if the attacker is already inside a network protected by proactive and reactive measures such as moving target defense, diversity, deception, and related technologies? We would be interested in justified new formulation to include discussion of the suggested formula and simulation results.

PNNL's Original Problem Set

Problem Statement
What is the best risk assessment model in order to support cyber resiliency?

Motivations
The work of security management is to ensure that risks are being assessed accurately in order to apply the proper measures and thus reduce the vulnerabilities on the network and reduce the risk thee information systems are exposed to while conducting business.

Methodology
Starting with an extensive analysis of the major risk assessment models, we are performing a deep dive analysis of their similarities and differences. Expand research to the less commonly used risk assessment models for a more complete analysis of risk assessment models.
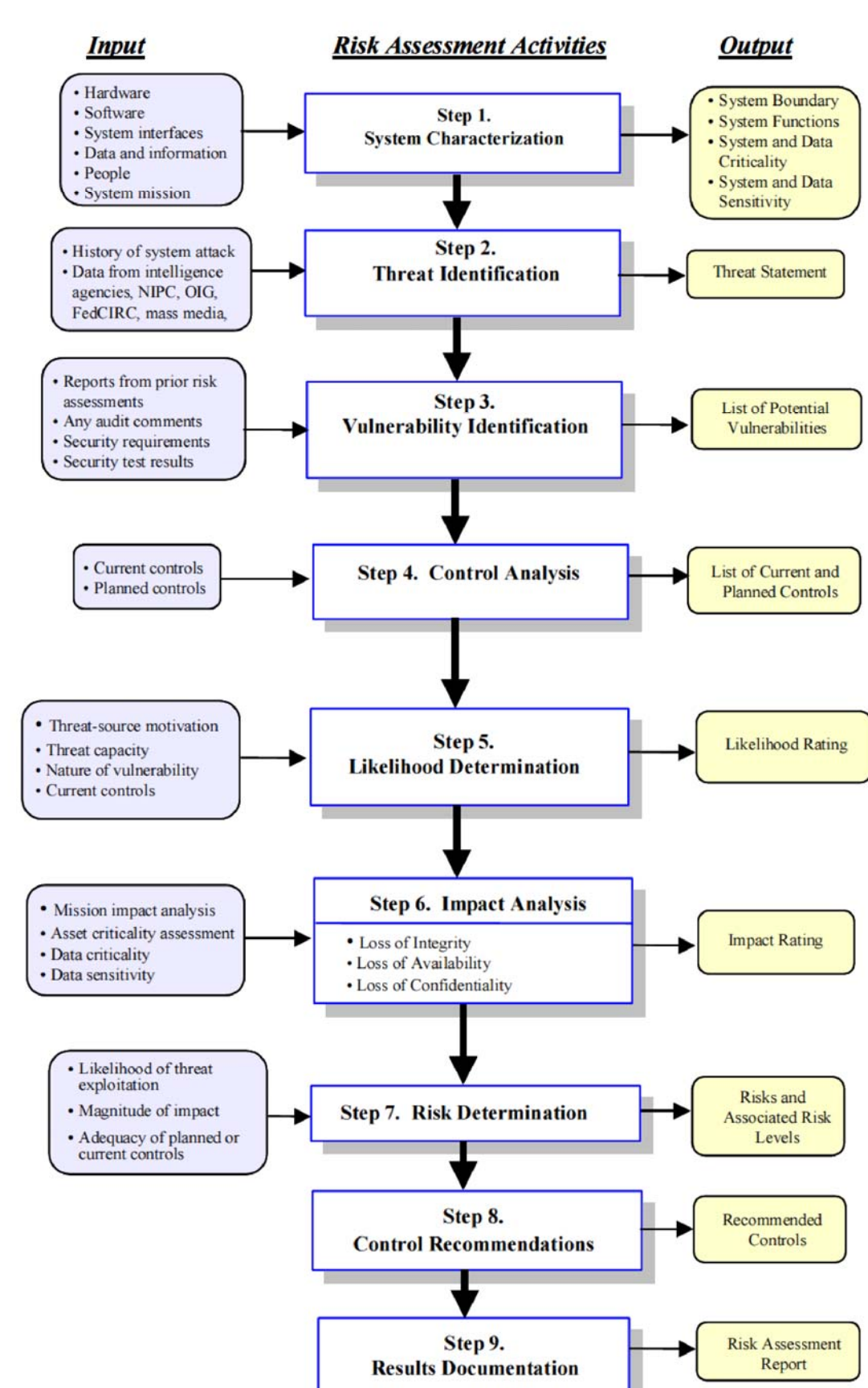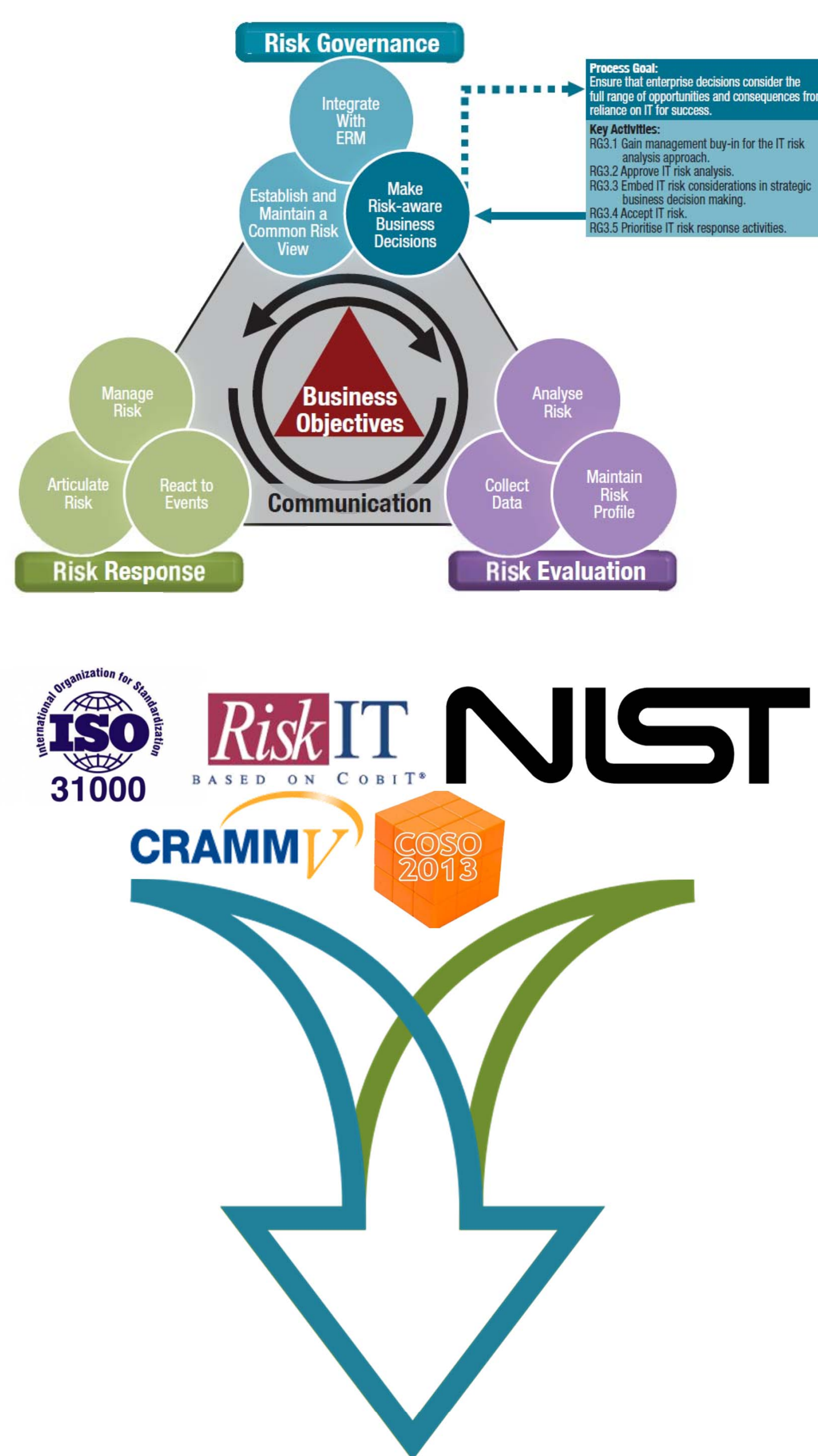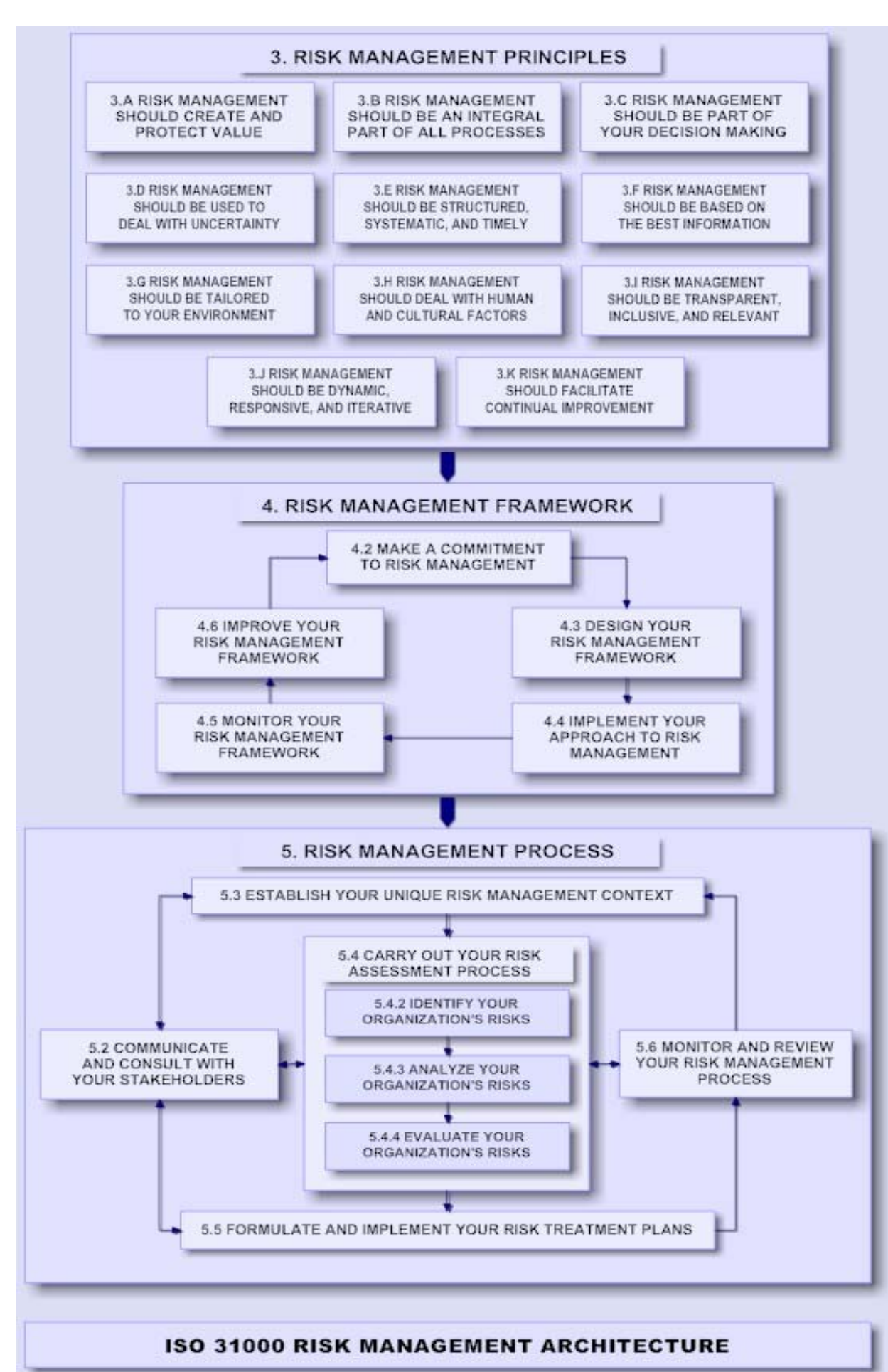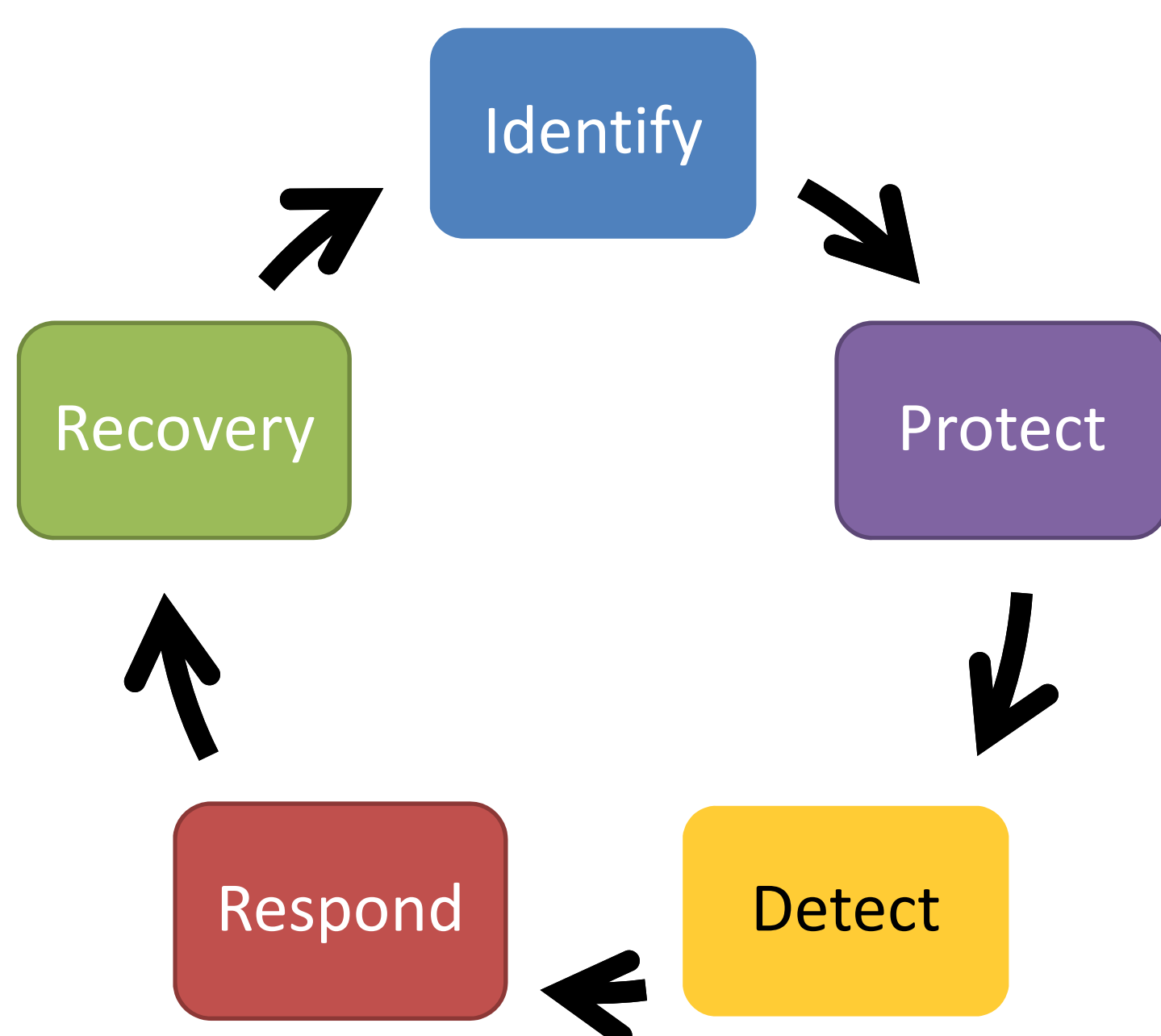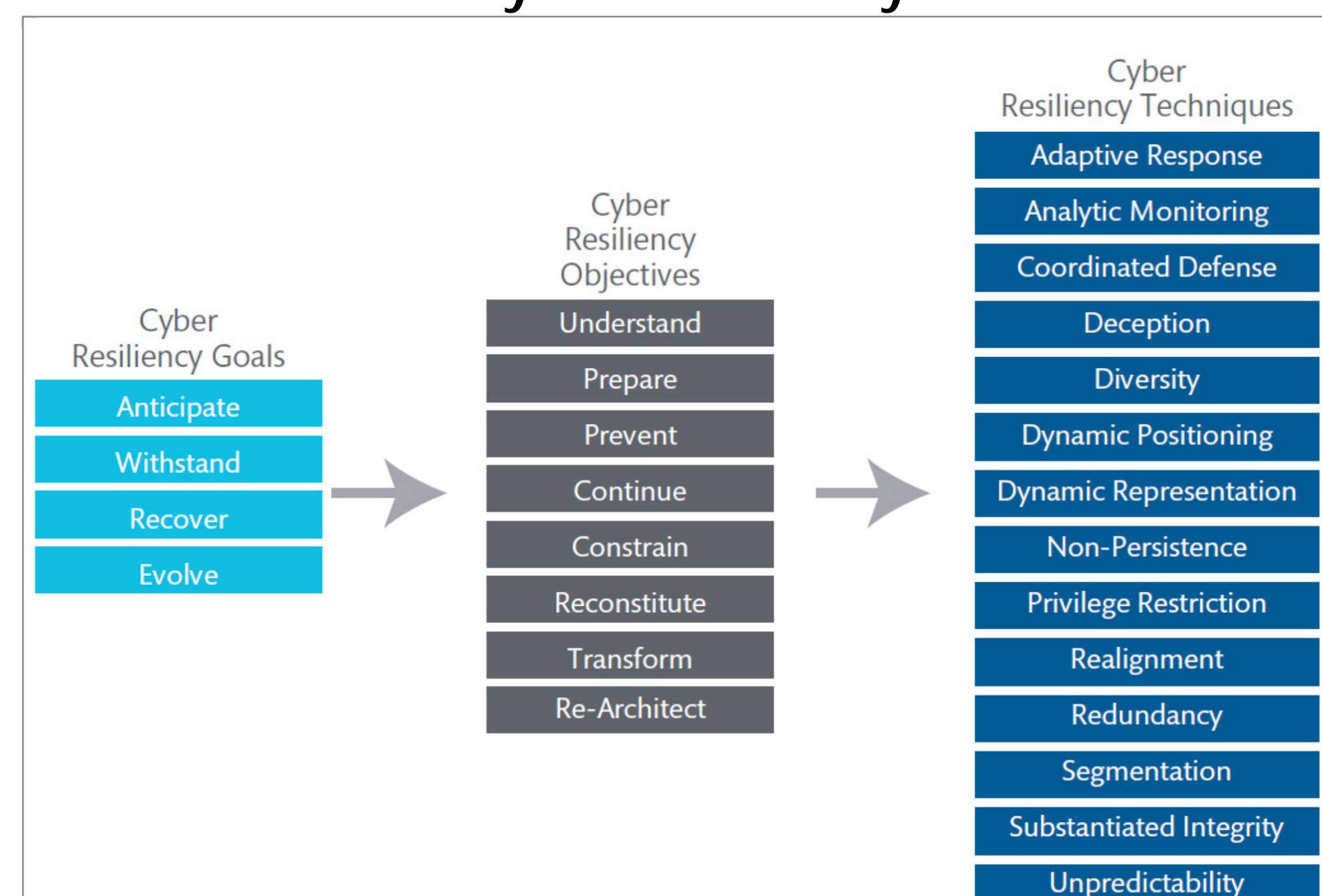

Figure 3-1. Risk Assessment Methodology Flowchart

NIST Cyber Resiliency Framework

MITRE Cyber Resiliency Model

Source: Jumpstart Resiliency with What You've Got (mitre.org)

INSuRE (http://insurehub.org) is training students in information security research with problems provided by the National Security Agency, Sandia National Labs, Pacific Northwest National Labs, and the Indiana Office of Technology. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the aforementioned."

CERIAS

PURDUE UNIVERSITY