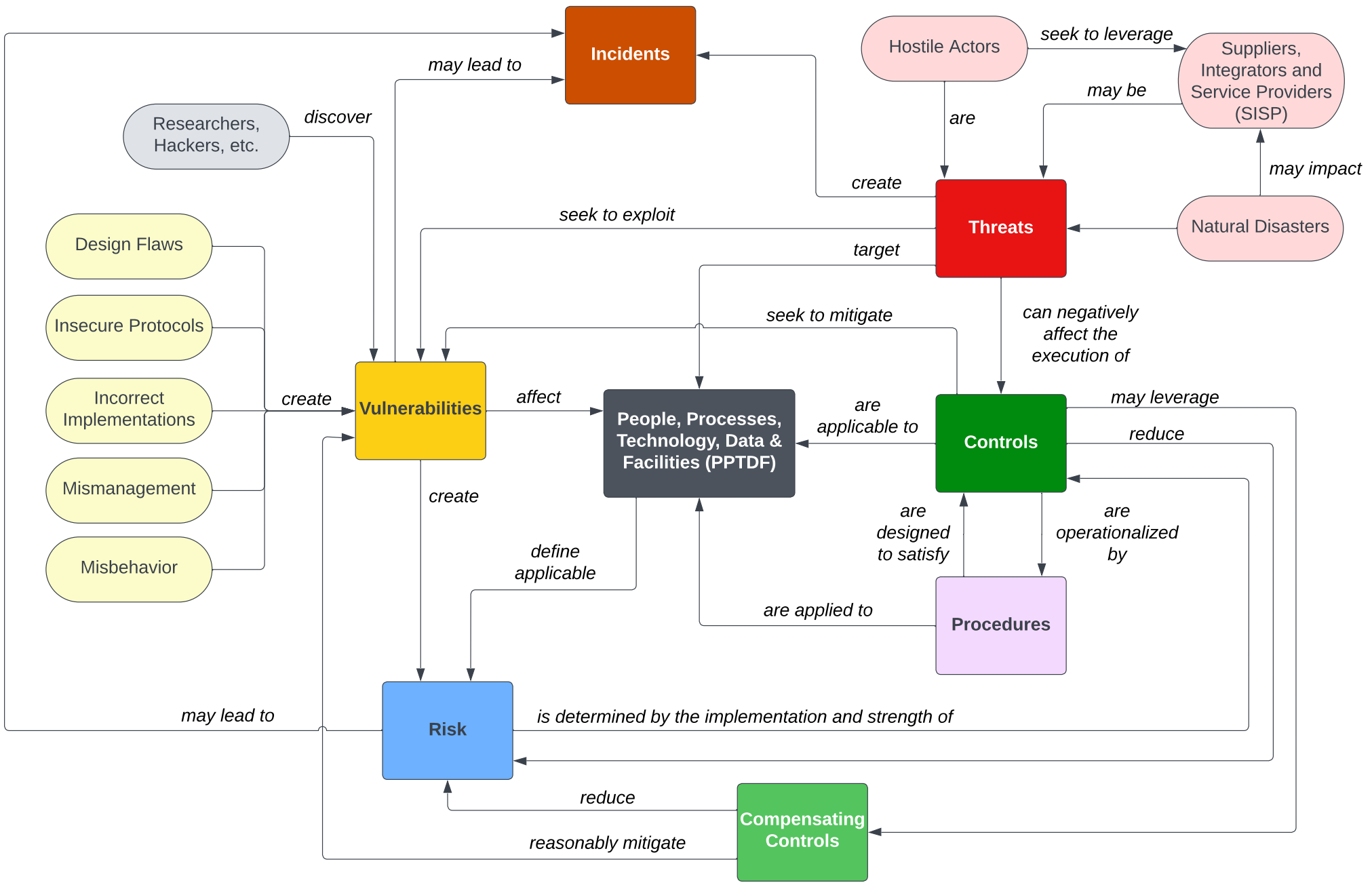
RISK ECOSYSTEM: THE INTERACTION OF RISKS, THREATS, VULNERABILITIES, CONTROLS & PROCEDURES

Threat, vulnerability and risk management practices are meant to achieve a minimum level of protection - this equates to a reduction in the total risk due to the protections offered by implemented controls. These ecosystem components have unique meanings that need to be understood to reasonably protect People, Processes, Technology, Data and Facilities (PPTDF). Understanding the context of how these components integrate can lead to more meaningful and practical risk management practices.

Key concepts associated with risk management include:

- Risk Appetite: Types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.
- Risk Tolerance: Level of risk an entity is willing to assume in order to achieve a desired result.
- Risk Threshold: Value used to establish concrete decision points and operational control limits to trigger management action and response escalation.



CONTEXTUAL DEFINITIONS

Threat

noun A person or thing likely to cause damage or danger.
verb To indicate impending damage or danger.

Risk

noun A situation where someone or something valued is exposed to danger, harm or loss.
verb To expose someone or something valued to danger, harm or loss.

Vulnerability

A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Control

The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

Compensating Control

The security controls employed in lieu of the recommended control(s) that provide equivalent or comparable protection for an information system or organization.

Procedure

A set of instructions used to describe a process or procedure that performs an explicit operation or explicit reaction to a given event. The design and implementation of a procedure must be reasonable and appropriate to address the control.

Reasonable

Appropriate or fair level of care. This forms the basis of the legal concepts of "due diligence" and "due care" that pertain to negligence.

Mitigate

To make less severe or painful or to cause to become less harsh or hostile.