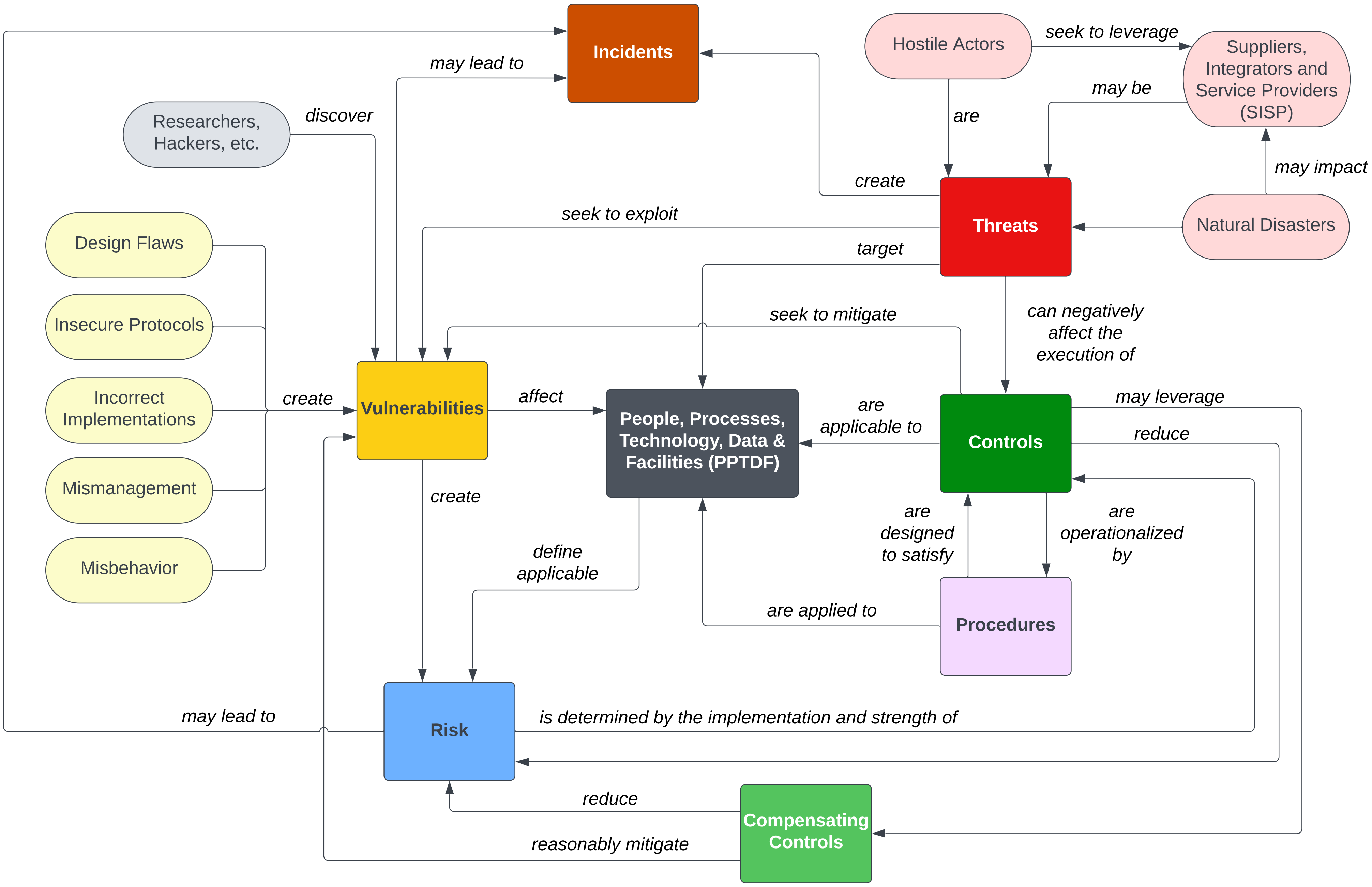
RISK ECOSYSTEM: THE INTERACTION OF RISKS, THREATS, VULNERABILITIES, CONTROLS & PROCEDURES

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 and data. Understanding the context of how these components integrate can lead to more meaningful and practical risk management practices.



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.

MATERIALITY ECOSYSTEM: THE INTERACTION OF MATERIAL CONTROLS, MATERIAL RISKS, MATERIAL THREATS & MATERIAL INCIDENTS

There is a "materiality ecosystem" that exists within modern cybersecurity risk management discussions. The process begins with determining what constitutes materiality for an organization. This is organization-specific and is primarily based on a clearly-defined financial threshold.

Defining materiality is an executive leadership determination, not a cybersecurity determination. Often, cybersecurity teams incorrectly hypothesize what "should be material" through the myopic perspective of the cybersecurity department. However, those cybersecurity-led definitions are often incorrect and are not material to the organization, much to the frustration of legal counsel that sometimes have to reprimand cybersecurity practitioners for incorrectly labeling incidents as material. For example, while a $5 million dollar incident may appear material (e.g., it is a significant sum), that financial amount may not come close to the actual materiality threshold for a prosperous organization.

Once the materiality threshold is clearly defined, it then requires a look at an organization's risk and threat management practices to identify those specific risks and threats that could lead to a material incident. Ideally, this means reviewing established risk and threat catalogs to identify known risks and threats that have material implications.

In the end, the due diligence activities performed to define material risk and material threats assist with broader incident response operations. This prior work assists the organization in defining material incidents, or at least pre-determined criteria associated with incidents, that would elevate incident response activities to the proper organizational leadership, due to the existence of a material incident (e.g., external reporting requirements, reputation damage control, etc.). During incident triage is not the correct time to develop incident threshold categories to determine materiality, due to requirements such as the US Securities and Exchange Commission (SEC) requires public companies to disclose material incidents within 72 hours.

COMPLIANCE FORGE

STEP 1: IMPACT ANALYSIS

Material Control. When a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control. A material control is such a fundamental cybersecurity and/or data protection control that:

- It is not capable of having compensating controls; and
- Its absence, or failure, exposes an organization to such a degree that it could have a material impact.

Material Risk. When an identified risk that poses a material impact, that is a material risk.

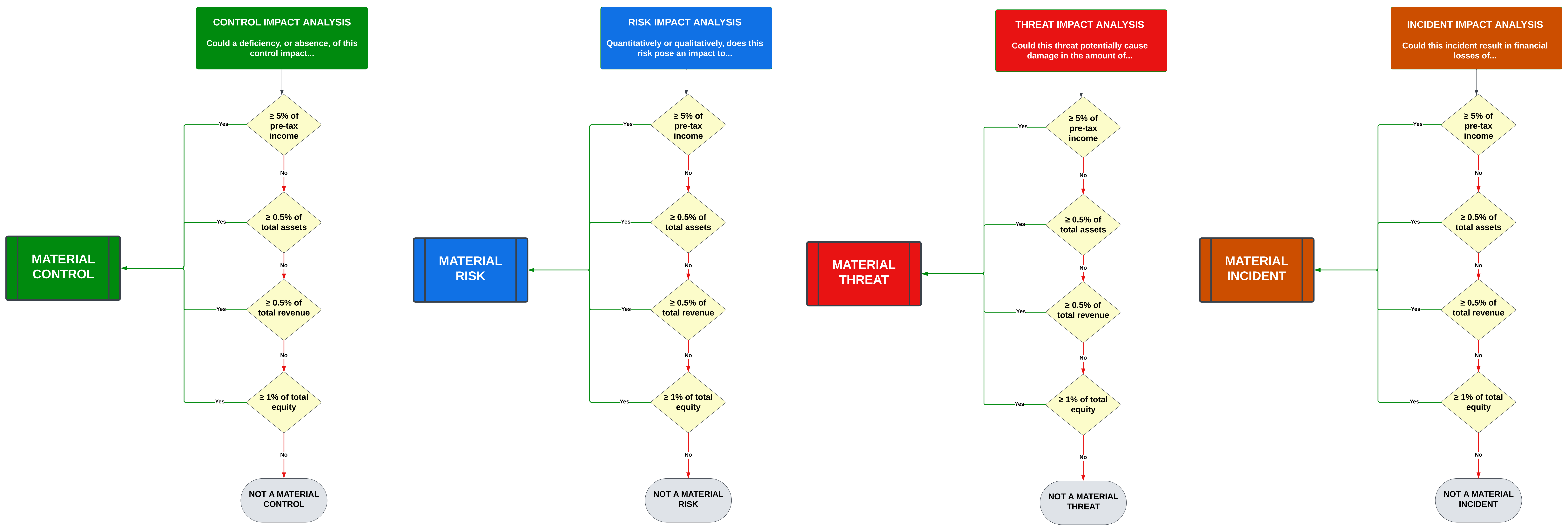
- A material risk is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., significant financial impact, potential class action lawsuit, death related to product usage, etc.); and
- A material risk should be identified and documented in an organization's "risk catalog" that chronicles the organization's relevant and plausible risks.

Material Threat. When an identified threat poses a material impact, that is a material threat.

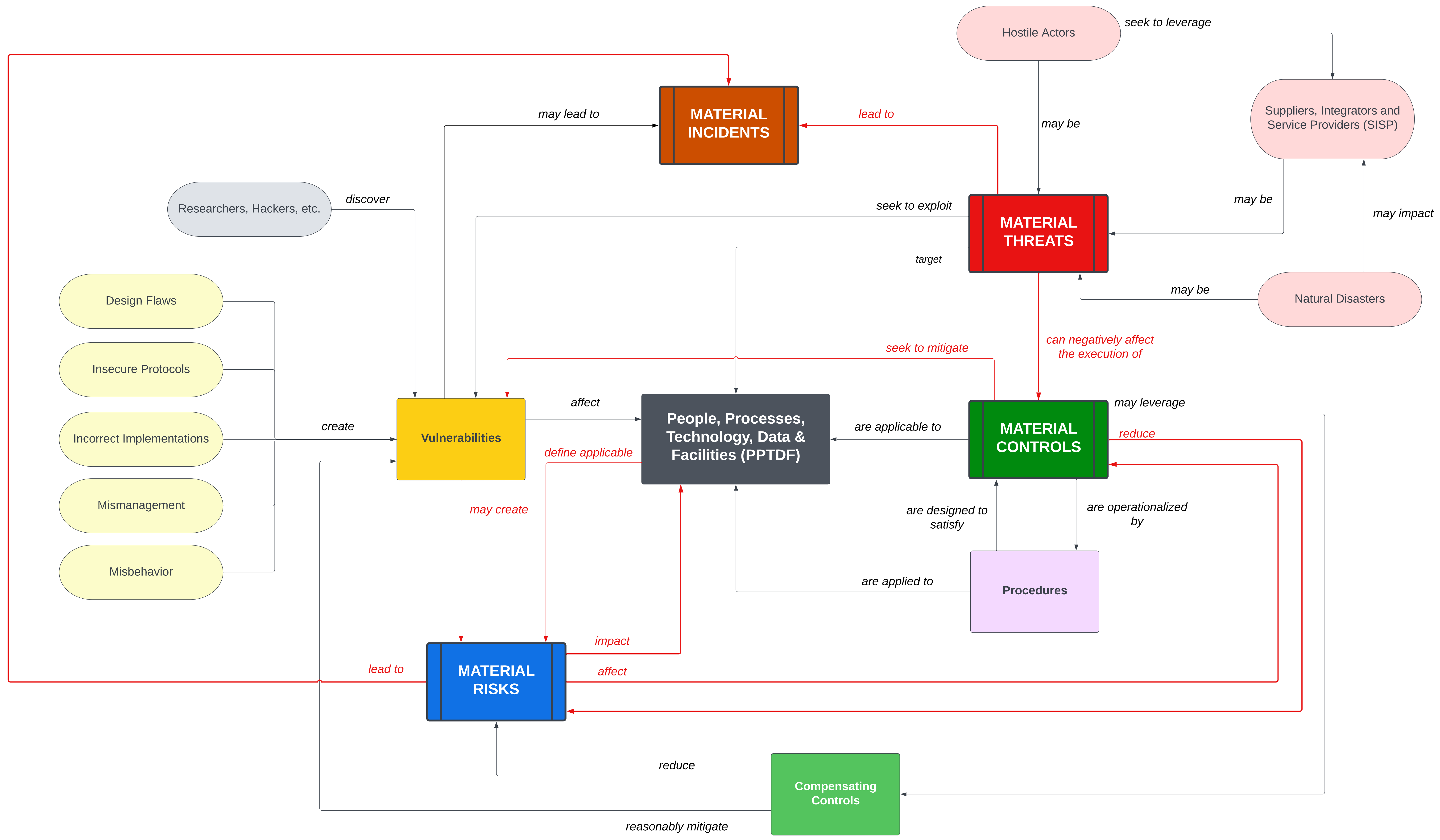
- A material threat is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and
- A material threat should be identified and documented in an organization's "threat catalog" that chronicles the organization's relevant and plausible threats.

Material Incident. When an incident poses a material impact, that is a material incident. A material incident is an occurrence that does or has the potential to:

- Jeopardize the Confidentiality, Integrity, Availability and/or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits with a material impact on the organization; and/or
- Constitute a violation, or imminent threat of violation, of an organization's policies, standards, procedures or acceptable use practices that has a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.).



STEP 2: UNDERSTANDING MATERIALITY RELATIONSHIPS TO BETTER GOVERN CYBERSECURITY OPERATIONS


Hostile Actors
seek to leverage
Suppliers, Integrators and Service Providers (SISP)
may be
may be
may impact
MATERIAL INCIDENTS
may lead to
lead to
Researchers, Hackers, etc.
discover
seek to exploit
MATERIAL THREATS
target
may be
Natural Disasters
Design Flaws
Insecure Protocols
Incorrect Implementations
Mismanagement
Misbehavior
create
seek to mitigate
can negatively affect the execution of
Vulnerabilities
affect
People, Processes, Technology, Data & Facilities (PPTDF)
are applicable to
MATERIAL CONTROLS
may leverage
reduce
define applicable
may create
are designed to satisfy
are operationalized by
are applied to
Procedures
impact
lead to
MATERIAL RISKS
affect
reduce
Compensating Controls
reasonably mitigate