Introduction to the FAIR Controls Analytics Model (FAIR-CAM)

Jack Jones

Chairman FAIR Institute

FAIR21 CONFERENCE

Ask yourself these questions…

- What's the most valuable control in your cybersecurity program?
- What's the least valuable control?

Would your answers be the same as someone else's in your organization?

Is it important to be able to answer these questions?

What do we mean by “value”?

The value proposition of any risk management control boils down to this:

Its ability to affect the frequency or magnitude of loss

Ask yourself these questions…

- How does patching reduce risk? How do you measure its effect?
- What about policies, awareness training, or logging?
- How does risk analysis reduce risk?

What’s been missing…

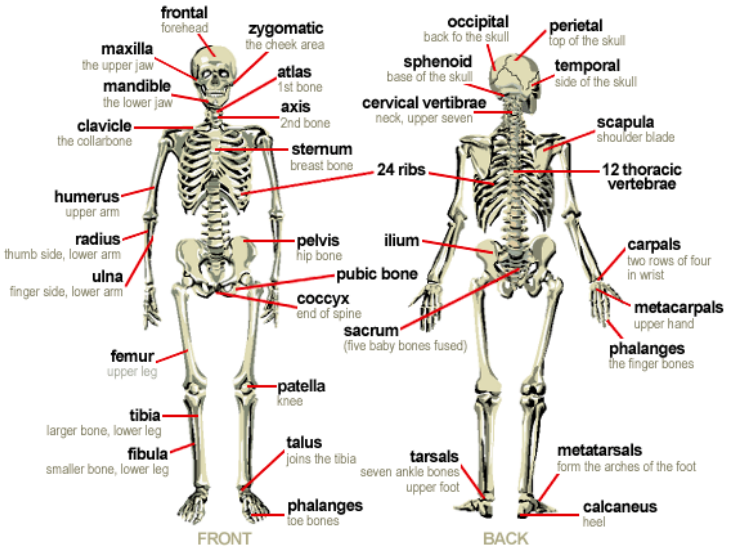
FAIR21 CONFERENCE

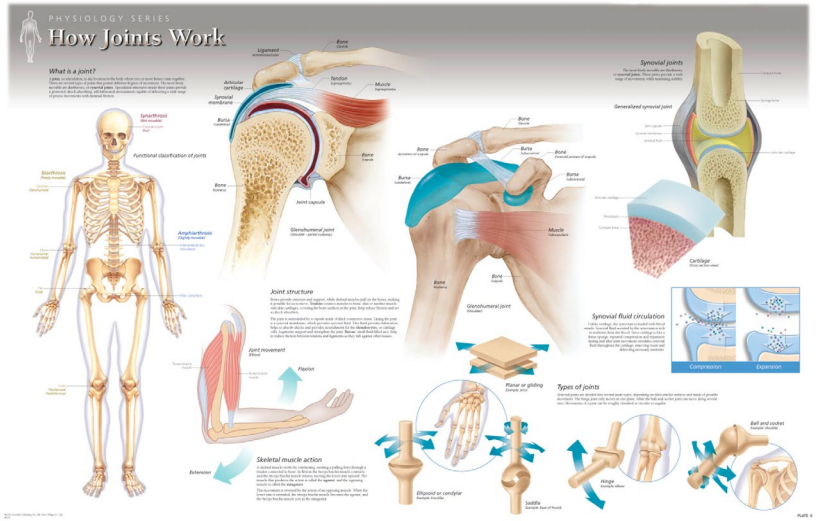
In the practice of medicine, which is more important?

Anatomy?
(The parts of the system)

OR

Physiology?
(How the system works)

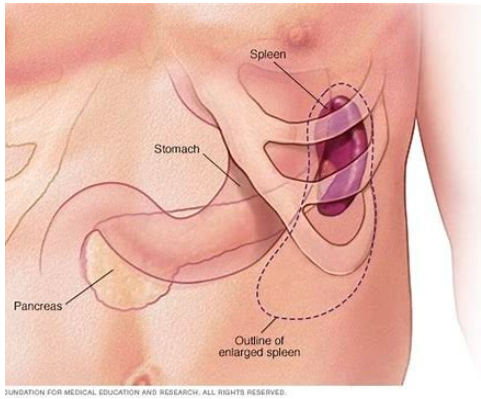




Neither. You need to know both.

Human Anatomy vs. Physiology

- **Anatomical component**: Spleen
  - Size: Approximately 1 x 3 x 5 inches
  - Weight: Approximately 7 oz
  - Location: Upper-left abdomen



- **Purpose**: Supports the immune system

- **Physiology**
  - Function: Blood filtering via white pulp and red pulp
  - Depends upon: Arteries, veins, nerves, lungs, etc…
  - Is depended upon by: Liver, brain, etc…
  - When missing or damaged is partially compensated for by: Lymph nodes, etc…

In other words, it's part of a system.

Cybersecurity Anatomy vs. Physiology

- **Anatomical component**: Awareness training
  - Content: Passwords, phishing, clean desk, etc.
  - Periodicity: Annual

- **Purpose**: Informs personnel of expectations

- **Physiology**
  - Function: Reduces the frequency of variant (i.e., deficient) control conditions
  - Depends upon: Policies, risk appetite, risk measurement, etc…
  - Is depended upon by: Authentication, system security, access privileges, physical security, data protection, etc…
  - When deficient, may be partially compensated for by: DLP, password enforcement, Anti-malware, etc.

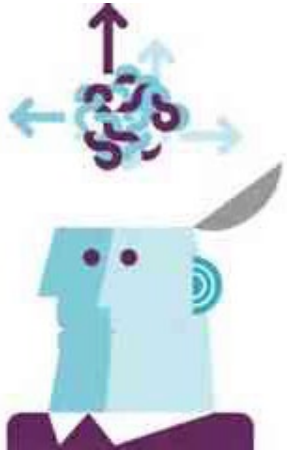
Example of cybersecurity “anatomy” (ISO27001)

A.9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

A.9.2.1	User registration and de-registration	*Control* A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
A.9.2.2	User access provisioning	*Control* A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
A.9.2.3	Management of privileged access rights	*Control* The allocation and use of privileged access rights shall be restricted and controlled.
A.9.2.4	Management of secret authentication information of users	*Control* The allocation of secret authentication information shall be controlled through a formal management process.
A.9.2.5	Review of user access rights	*Control* Asset owners shall review users’ access rights at regular intervals.
A.9.2.6	Removal or adjustment of access rights	*Control* The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

But, how controls function, and function together, to reduce risk has been mostly undefined, leaving us to rely on…



Mental models

FAIR Controls Analytics Model (FAIR-CAM)

FAIR-CAM Objectives

- Describe controls physiology so that we can:
  - Bridge the gap between controls “anatomy” and risk
  - Properly account for individual control functionality as well as systemic functionality
  - Reliably forecast, measure, and validate control efficacy and value
  - Enable better use of security telemetry
  - Evaluate program maturity more effectively
- Become an industry standard
  - Anticipate that this will be covered under a creative commons Attribution-Non Commercial-No Derivative license, similar to how the Open Group and CIS protect their work
    - Licensing and exemption processes will be available

Setting expectations…

Modern medicine is complex because human physiology and pathology are complex.

If we want to effectively manage a problem space like cybersecurity, we have to account for its complex nature.

There is no easy button for cybersecurity.

Clarifying terms

Controls:
"Anything used to directly or indirectly affect the frequency or magnitude of loss."

Examples:
Policies
Passwords
Patching
Data backups
Auditing
etc…

Control Functions:
"How a control directly or indirectly affects the frequency or magnitude of loss."

Examples:
Loss Event Prevention
Loss Event Detection
Variance Prevention
Variance Correction
etc…

Current controls functions in the industry?

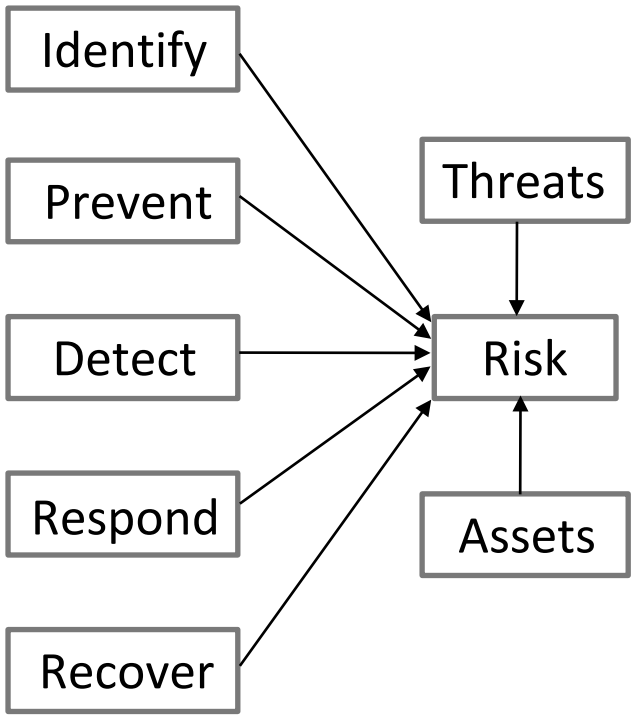
Problems include, but aren't limited to:

- Doesn't differentiate between functions that directly vs. indirectly affect risk (commonly inferred that all controls affect risk directly)
- Doesn't account for dependencies between controls
- Not granular enough to enable accurate or verifiable measurement of control efficacy or value

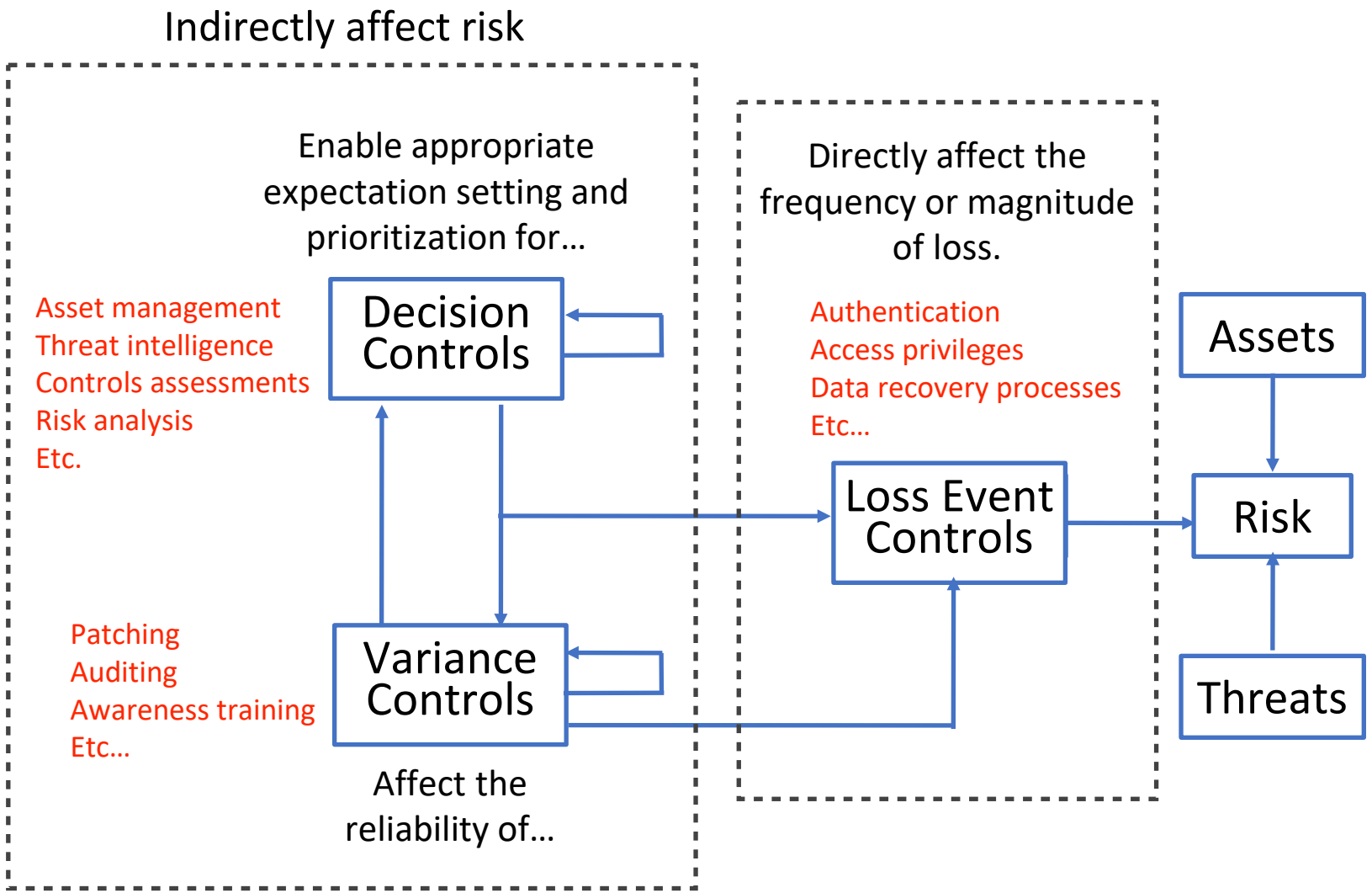
NOTES:

- NIST 800-53 mentions that controls are "related", but does not define the nature of the relationships.
- "Threat Kill Chain" analysis is somewhat similar in principle, but has a very narrow scope, focuses only on a subset of controls, and doesn't account for control relationships.

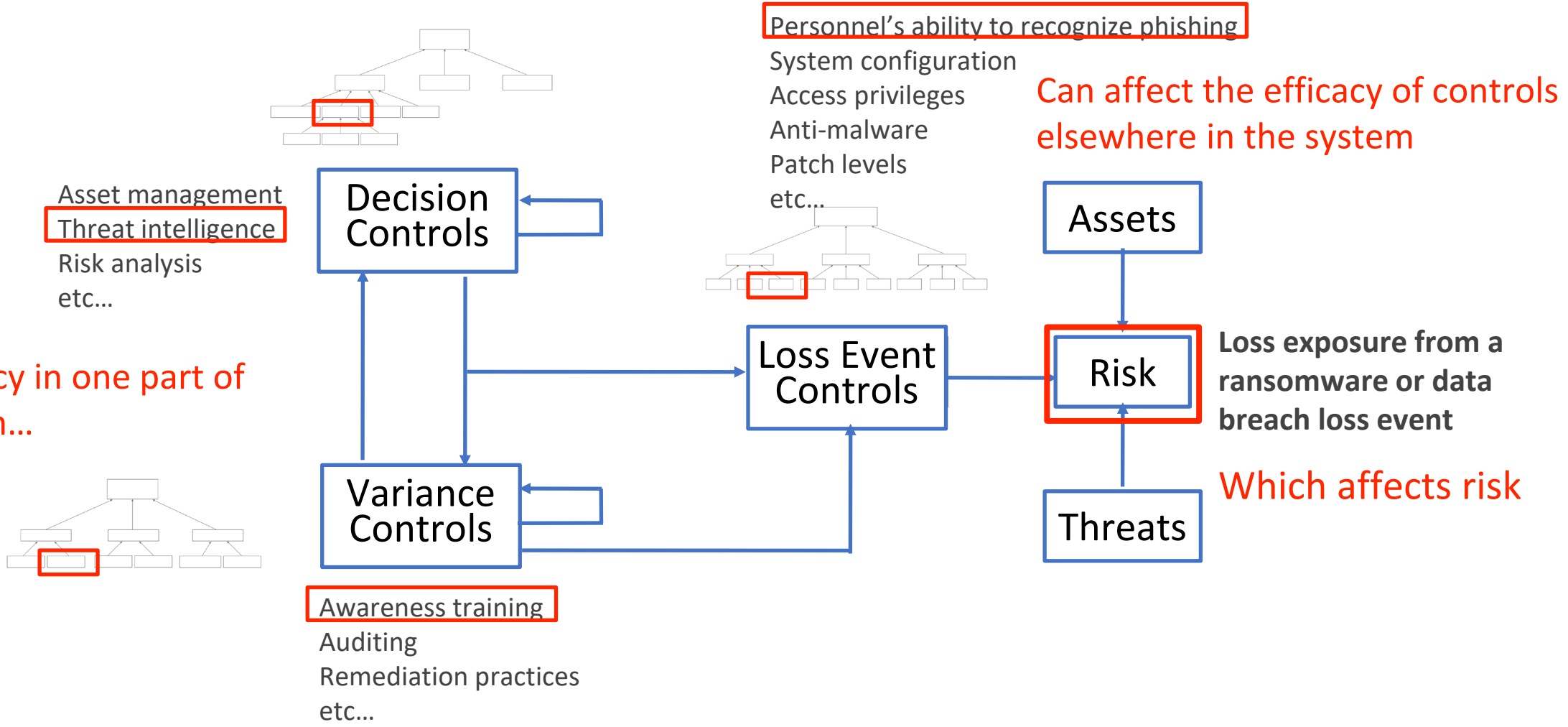
Control Functions
(NIST CSF)



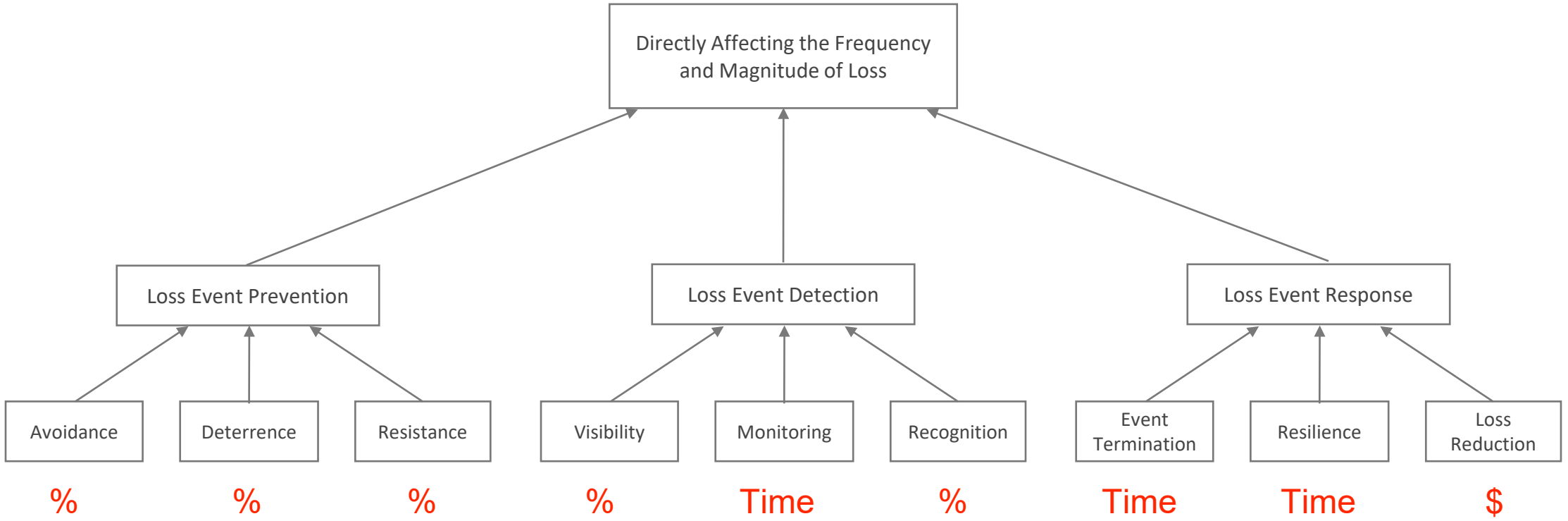
Control Functional Domain Relationships



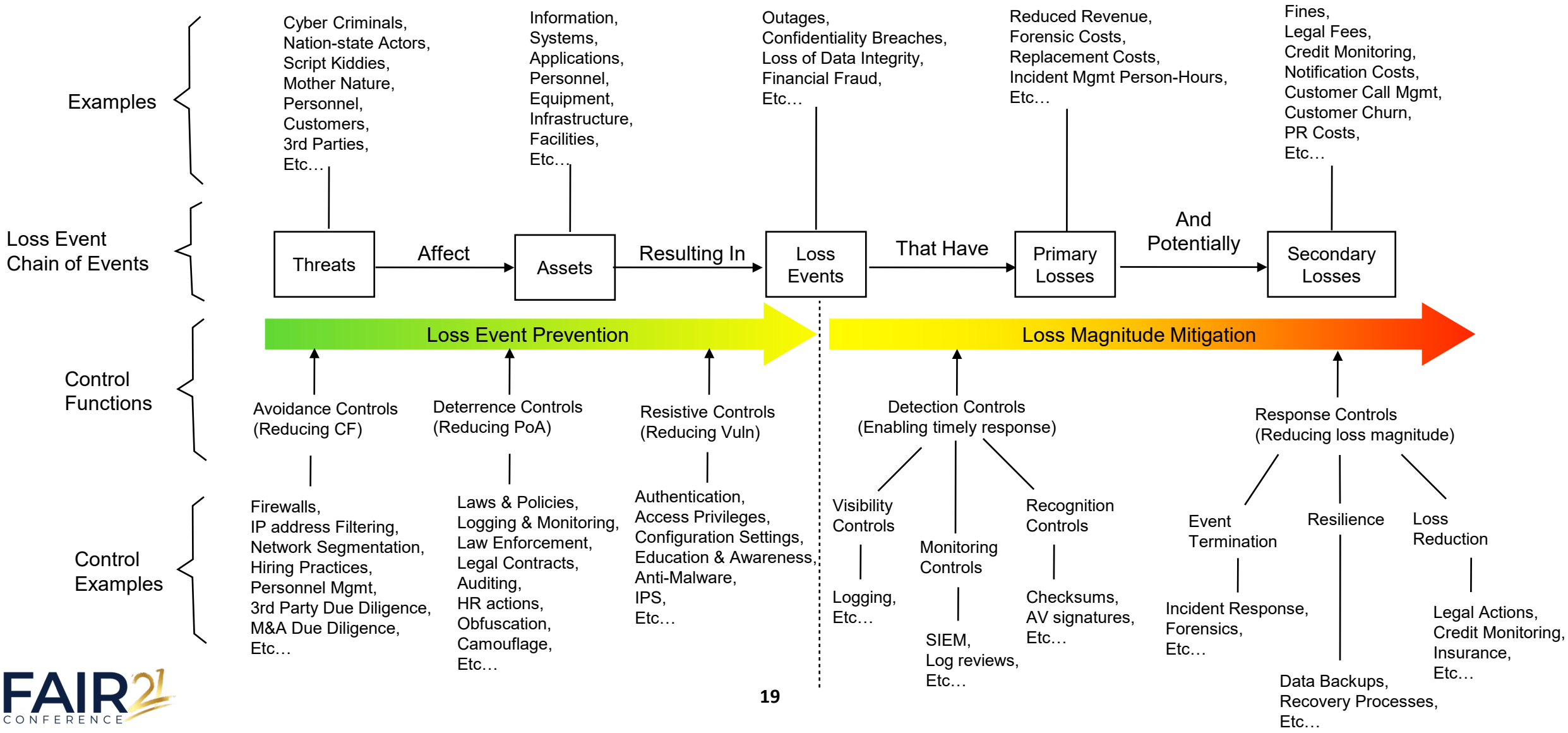
Control Functional Domain Relationships



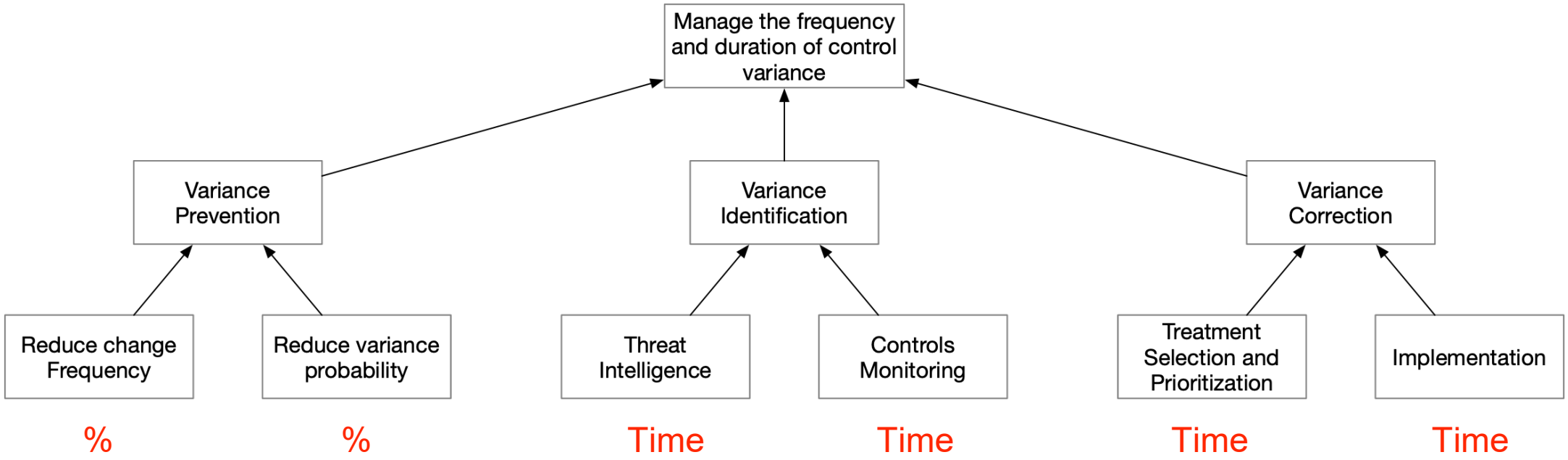
Loss Event Control Functions



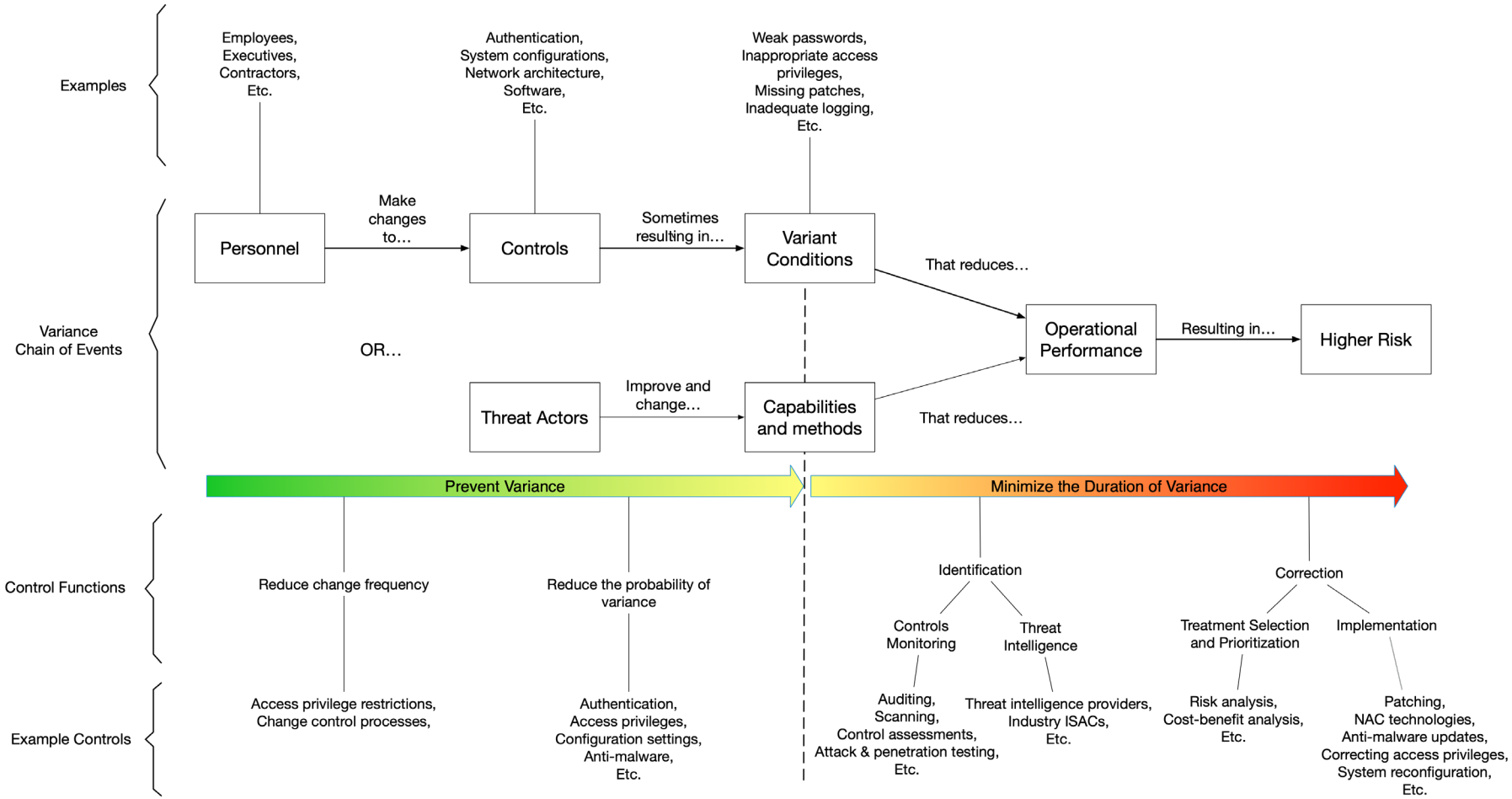
Loss Event Controls applied to risk



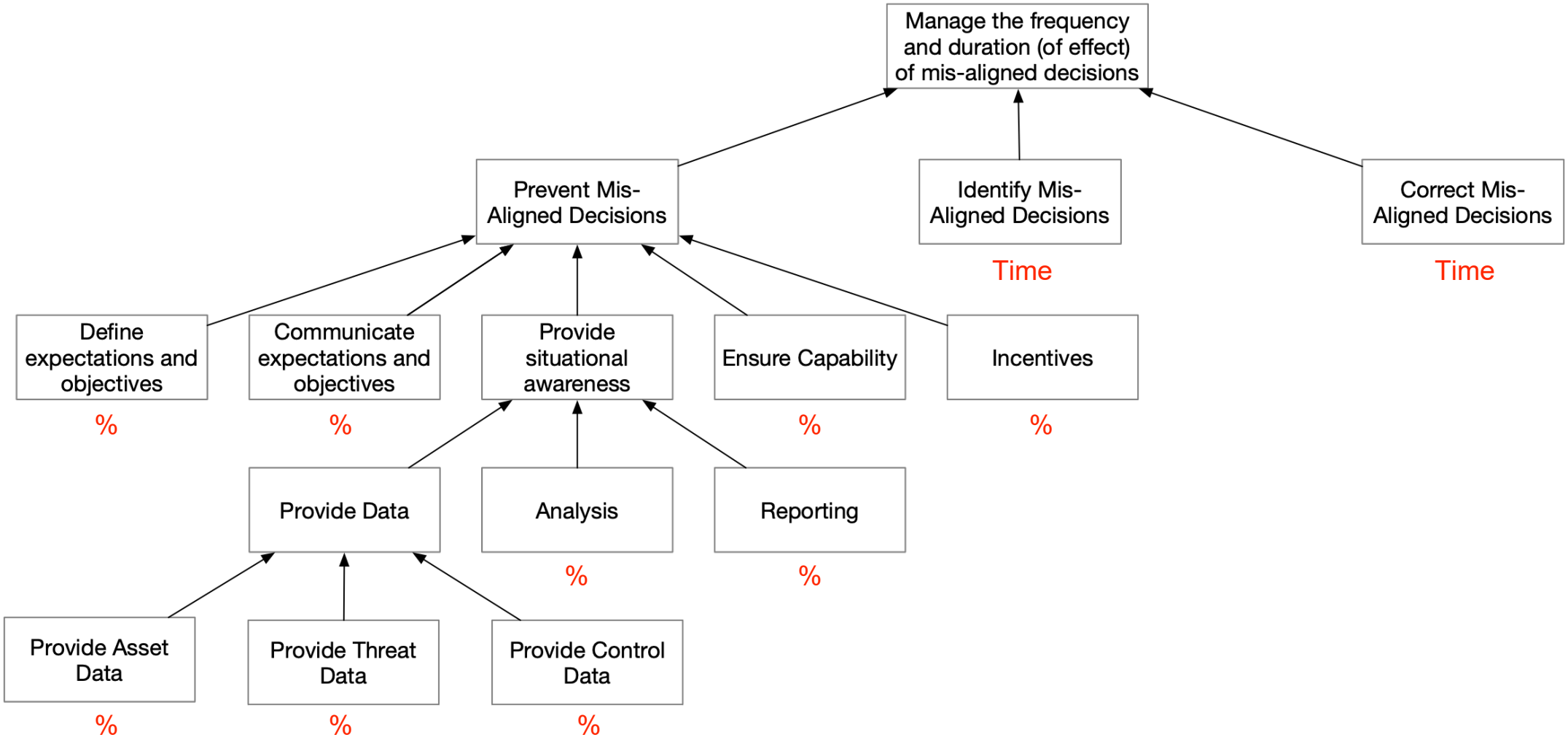
Variance Management Control (VMC) Functions



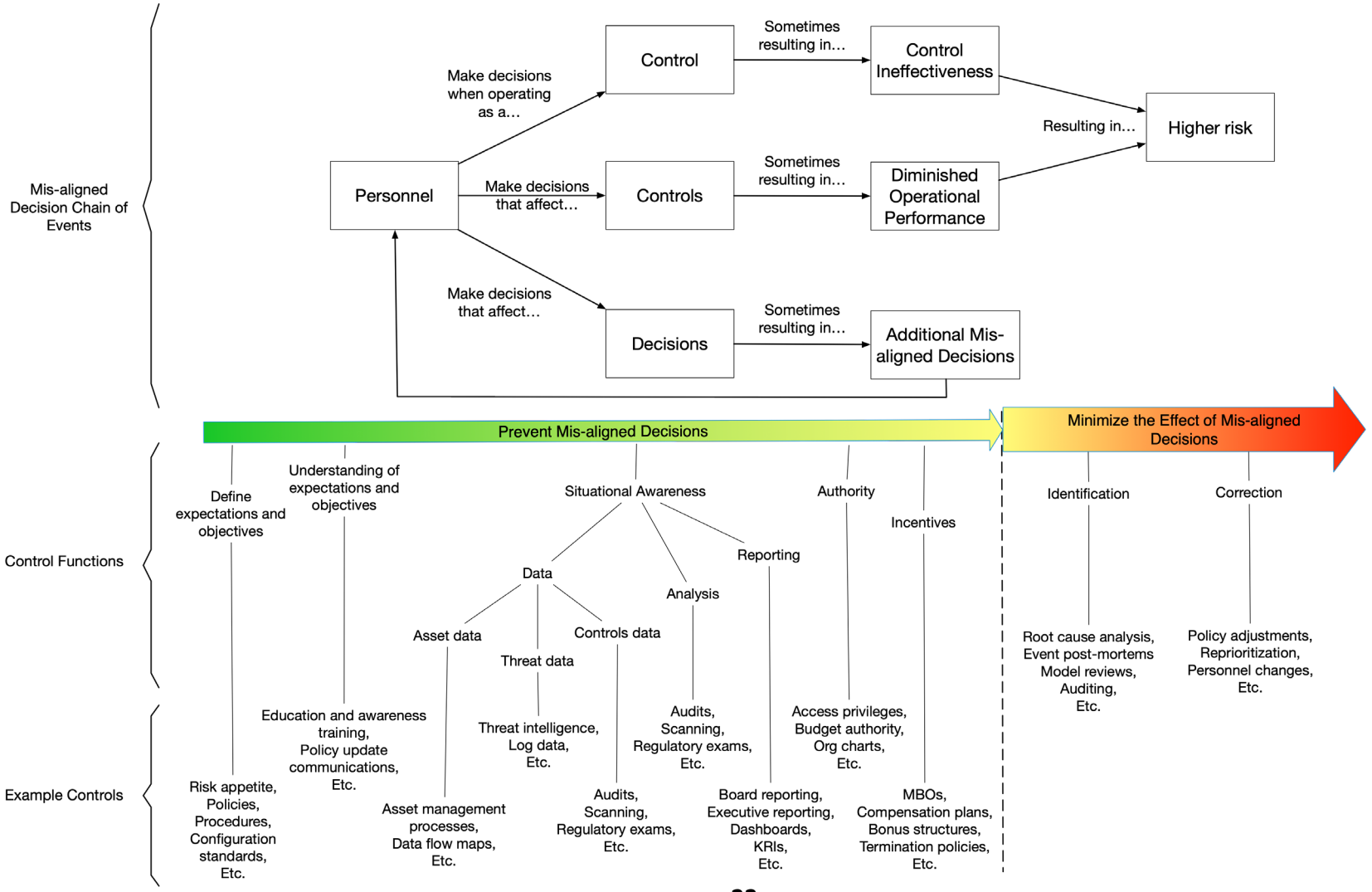
Variance Management Controls affect on risk



Decision Support Control (DSC) Functions



Decision Support Controls affect on risk



Combining controls “anatomy” with “physiology”

The objectives...

- Clarify how framework elements affect risk
- Make it easier to apply control frameworks within risk analysis
- Enable more reliable prioritization of control gaps
- Enable the refinement of control frameworks

Current mapping efforts…

- ISO27k
- CIS v8.0
- NIST 800-53
- HITRUST

Future mapping efforts…

- Mitre Att&ck
- COBIT
- PCI-DSS
- Others as requested

Wrapping up…

FAIR21 CONFERENCE

Summary

- Current control frameworks provide a view of control “anatomy” but rely on practitioner mental models to deal with “physiology”.
- As a result, we are unable to reliably measure or prioritize our control efforts.
- FAIR-CAM provides a “controls physiology” view, which complements existing frameworks and fills a critical gap in our ability to manage risk effectively.
- When FAIR-CAM is combined with FAIR, we can measure control value in real terms and reliably prioritize where and how we apply our resources.

"In the 19th century we had a relatively advanced understanding of anatomy, but we had a terrible understanding of physiology.

We knew what was happening, but we didn't know why it was happening."

A retired surgeon

Resources

- Documents
  - Introduction to the FAIR Controls Analytics Model
  - Description of the FAIR Controls Analytics Model Standard [DRAFT]
  - Applying the FAIR Controls Analytics Model Coming soon…
  - CIS 8.0 to FAIR-CAM Mapping
  - Various other mapping documents… Coming soon…
- Training & Certification
  - Basic FAIR-CAM Under development…
  - Advanced FAIR-CAM Under development…
- Software
  - FAIR-CAM enabled prototype in development

Questions?

FAIR21 CONFERENCE