FAIR Controls Analytics Model (FAIR-CAM™)

Standard Artifact | Version 1.0

January 15, 2025

www.FAIRInstitute.org

Table of Contents

1 | Introduction

NOTE: Before reading this document, it is highly recommended that you read the Introduction to the FAIR Controls Analytics Model (FAIR-CAM™) white paper, which is available here on the FAIR Institute website. Also, it is assumed that readers of this document are already familiar with the basics of Factor Analysis of Information Risk (FAIR).

1.1 | Overview of FAIR-CAM

The FAIR Controls Analytics Model (FAIR-CAM) provides a rigorous description of how the risk management controls landscape works. It achieves this by describing the controls landscape as a complex set of interdependent functions that act as a system in the management of risk. This is analogous to how human physiology describes the way in which the different parts of the body operate as a system. This "controls physiology" view fills a void in how risk management has historically been practiced, which has focused almost exclusively on the parts of the system (the controls) versus how those parts operate as a system.

This controls physiology model complements, rather than displaces, frameworks such as ISO27001, NIST CSF, NIST 800-53, and HITRUST CSF. In fact, when combined with control frameworks such as those, as well as the FAIR model for risk measurement, FAIR-CAM enables much more reliable measurement, analysis, forecasting, and empirical validation of control efficacy and value.

This document focuses on describing the model itself — the parts that make it up and how they are organized. For an introduction to the model's underlying principles, please refer to the Introduction to the FAIR Controls Analytics Model (FAIR-CAM) white paper. For information on how to apply the model when performing risk analyses, please refer to the *Applying the FAIR Controls Analytics Model (FAIR-CAM)* white paper. Both of these documents are (or soon will be) available on the FAIR Institute website.

1.2 | Licensing and Use

The FAIR-CAM ontology is intended to serve as an international standard for controls physiology. In order to support this objective, this work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode. To further clarify the Creative Commons license related to FAIR-CAM content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization, for non-commercial purposes only, provided that (i) appropriate credit is given to the FAIR Institute, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the FAIR Controls Analytics Model, you may not distribute the modified materials. Users of the FAIR-CAM are also required to refer to http://www.fairinstitute.org/FAIR-CAM/ when referring to the model in order to ensure that users are employing the most up-to-date guidance. Commercial use of FAIR-CAM is subject to the prior approval of the FAIR Institute.)

1.3 | Terminology

As is the case with many professional disciplines, terms can have different meanings to different people. Therefore, in order to avoid confusion, this section provides definitions for three terms that are key to understanding, applying, and communicating about FAIR-CAM.

1.3.1 | Control

"Anything that can be used to reduce the frequency or magnitude of loss."

Controls can be laws, regulations, policies, standards, processes, technologies, people, software, physical structures, or anything that can be used to reduce risk. This definition is intentionally broad in scope, as it enables us to account for the risk reduction effects of more things.

1.3.2 | Control Function

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

A few examples of how controls can affect risk include:

- Limiting contact with threats (threat avoidance)
- Making it more difficult for threats to adversely affect assets (loss event resistance)
- Providing evidence that a loss event has occurred (loss event visibility)
- Restoring operations after an outage-related loss event has occurred (loss event resilience)
- Reducing the frequency of missing or deficient controls (variance prevention)
- Detecting that controls are missing or in a deficient condition (variance identification)
- Risk analysis (situational awareness)

1.3.3 | Functional domains

"High-level categories of control functions"

Functional domain categories distinguish between control functions that affect risk directly (Loss Event Controls), versus those that affect the Operational Performance of controls (Variance Management Controls), versus those that affect decision-making (Decision Support Controls).

2 | Model Description

This section of the document describes the current FAIR-CAM standard. The first subsection provides a description of the three functional domains defined within FAIR-CAM. This is followed by subsections that describe the control functions within each domain. These descriptions include:

- The function's role within its functional domain
- The function's relationship to other control functions
- Examples of common controls that perform the function
- The unit of measurement for control performance

2.1 | Function Relationships

A unique property of the FAIR-CAM ontology is that it describes and accounts for the relationships between control functions. In some cases, these relationships are dependencies — i.e., the benefits of one control function can't be realized unless another control function is operating as well. In Boolean logic, this is referred to as an AND relationship. A simple example is loss event detection. In order to detect that a loss event has occurred, you have to have access to data that would provide evidence of an event, AND you have to review that data — i.e., the data has to exist and the review has to occur in order for an event to be detected.

In other cases, the relationship is such that if even just one of two or more control functions is successfully performed, the risk management objective will be achieved — i.e., it only takes one functioning control to have the desired effect. In Boolean logic, this is referred to as an OR relationship. A simple example is loss event prevention. If you can (a) prevent contact with a threat agent, (b) deter action on the part of the threat agent, or (c) successfully resist the actions of a threat agent, then a loss event will not occur.

In still other cases, relationships exist where some controls improve the performance of other controls. For example, when a human being is acting as a loss event resistive control (e.g., when they encounter phishing emails), their efficacy in performing this function is improved by education and awareness training, which is a different control.

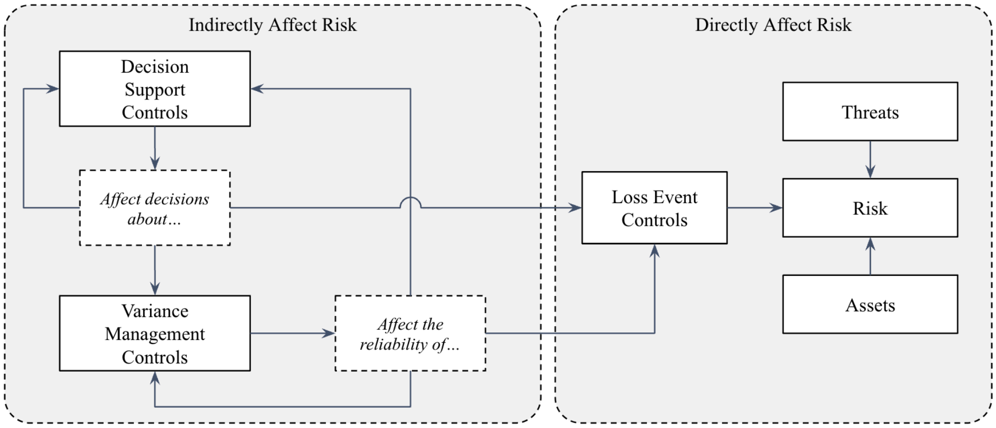
Consequently, in order to understand the efficacy of an organization's risk management program, you have to understand not only the controls that are in place but also the functions those controls serve and the dependencies between those functions.

2.2 | The Functional Domains

There are three distinct ways in which controls affect risk:

- By directly affecting the frequency or magnitude of loss (Loss Event Control functions)
- By affecting the reliability of controls (Variance Management Control functions)
- By affecting decisions (Decision Support Control functions)

Recognizing these distinctions provides a structure for how controls affect risk, which lays the foundation for reliable measurement. The diagram below provides a high-level illustration of how these domains relate to one another in risk management.


Indirectly Affect Risk
Directly Affect Risk
Decision Support Controls
Affect decisions about...
Variance Management Controls
Affect the reliability of...
Loss Event Controls
Threats
Risk
Assets

Note that both Variance Management Controls and Decision Support Controls affect risk indirectly through their effect on Loss Event Controls. Note also that Variance Management Controls can affect not only the reliability of Loss Event Controls but also Decision Support Controls and even other Variance Management Controls. Likewise, Decision Support Controls affect decision-making about Loss Event Controls, Variance Management Controls, and even other Decision Support Controls.

The definitions for these functional domains, as well as their structures, are described in the sections that follow.

2.3 | Common Dependencies

The Operational Performance of any control within any of the functional domains is dependent upon the frequency and duration of deficiencies in the control. As a result, you should assume that all controls are to some extent dependent upon Variance Management Controls. Similarly, because decisions inherently affect all controls in some manner, you should assume that all controls are dependent upon Decision Support Controls.

For example, Anti-malware technologies primarily fulfill Loss Event Control functions (Resistance, Detection, etc.), yet their efficacy in fulfilling those functions is dependent upon how frequently and for how long it's operationally deficient, which is driven by the Variance Management Controls (e.g., auditing, updating, etc.) that are applied to it. Decisions regarding which Anti-malware product to use, as well as policies and processes for how to operate and manage it, are affected by Decision Support Controls (e.g., policies, situational awareness, etc.).

Because of the inherent dependencies all controls have on VMCs and DSCs, this document will not explicitly describe those dependencies, as that would be redundant.

2.4 | Measuring Control Operational Effectiveness (Maturity)

Capability, Coverage, and Reliability are the critical attributes for evaluating the Operational Effectiveness of controls (i.e., Control Maturity), particularly in the context of the FAIR Controls Analytics Model (FAIR-CAM). These attributes are central to understanding and quantifying how well controls mitigate risk.

2.4.1 | Capability

A control's inherent ability to perform its intended function in addressing specific aspects of risk. This considers the design and expected effectiveness of the control. Key attributes of Capability include:

- The extent to which the control is designed to reduce risk (e.g., preventing, detecting, or responding to threats) and its technical and procedural design quality.
- How well it functions per its design in real-world scenarios and workloads.
- Its alignment with (or outperformance against) industry best practices and standards.

For example, an antivirus program's ability to detect malware based on its signature database is a measure of its capability.

2.4.2 | Coverage

Measures the extent to which a control or set of controls applies to the assets, threats, or risk scenarios within the organization. It reflects the breadth of a control's deployment or application. Key attributes include:

- The scope of assets, processes, or threat scenarios the control addresses.
- Its deployment footprint across systems, networks, or organizational processes.
- Gaps in coverage where the control is absent or ineffective.

For example, a firewall deployed across all internet-facing servers has broad coverage, while one protecting only a subset of servers has limited coverage.

2.4.3 | Reliability

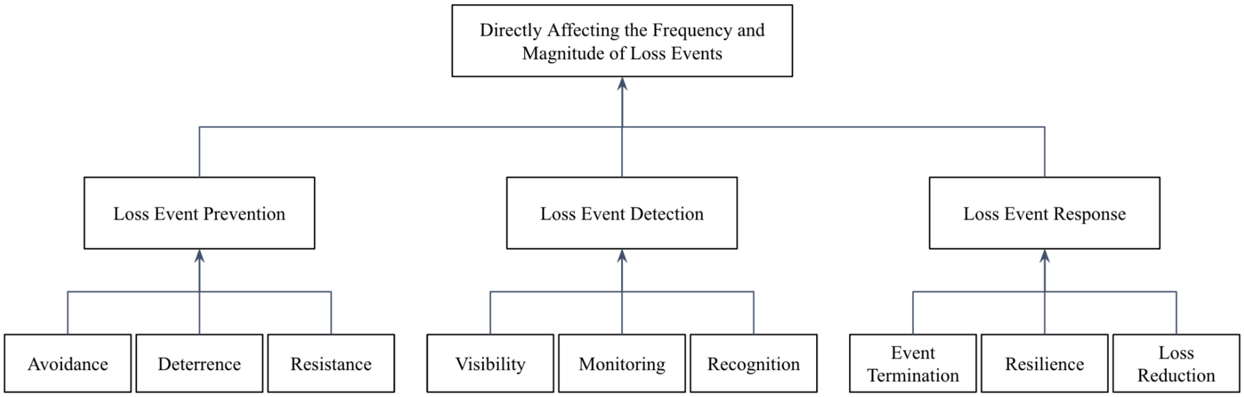
Refers to the likelihood that a control will perform its intended function consistently and without failure when needed. This considers both operational reliability and resilience to environmental or systemic issues. Key attributes include:

- The stability and resilience of the control over time.
- Its operational performance under varying conditions or stress.
- The likelihood of failure due to poor maintenance, misconfiguration, or other factors.

For example, a backup system with regular testing and validation has higher reliability compared to one without consistent monitoring.

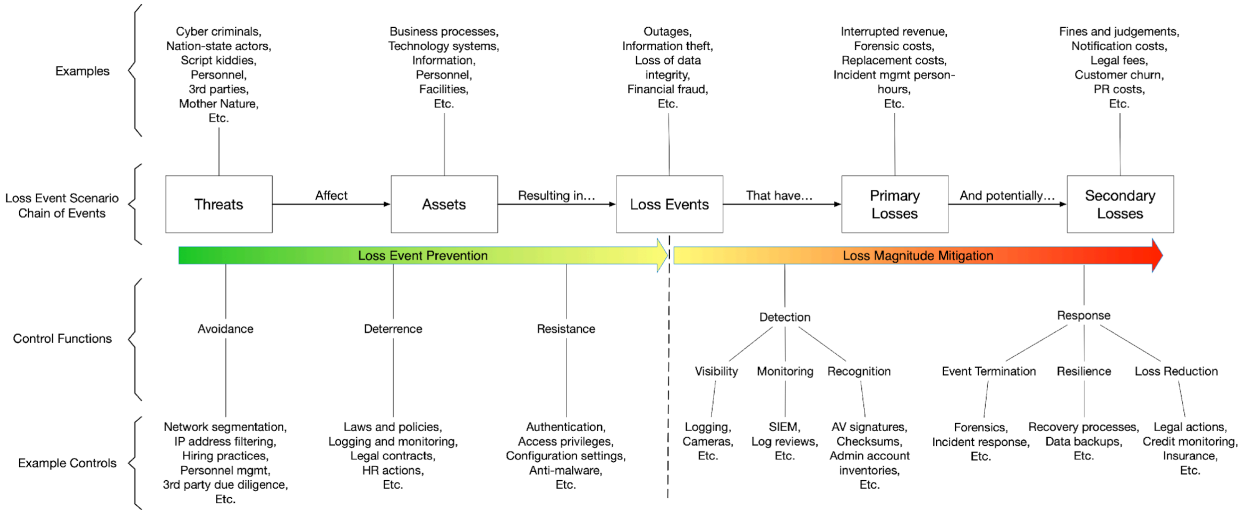
3 | The Loss Event Control (LEC) Functional Domain

As implied by its name, controls within this domain directly affect the frequency or magnitude of loss events. The diagram below illustrates the ontology for this domain:

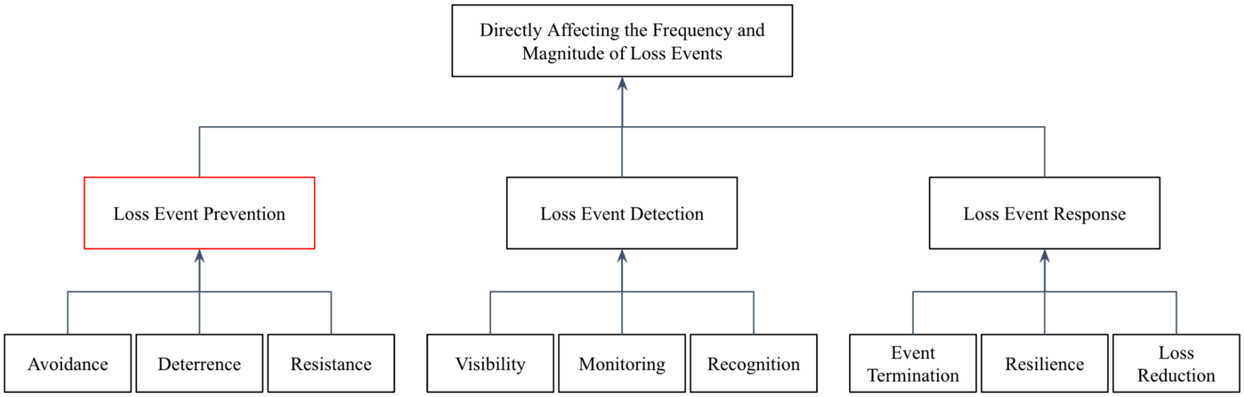


It is worth noting that Loss Event Detection and Loss Event Response have a Boolean AND relationship to one another — i.e., both must exist in order to mitigate the effects of a loss event.

The diagram below illustrates how these control functions affect risk and provides some examples of controls that perform those functions.


Examples
Cyber criminals, Nation-state actors, Script kiddies, Personnel, 3rd parties, Mother Nature, Etc.
Business processes, Technology systems, Information, Personnel, Facilities, Etc.
Outages, Information theft, Loss of data integrity, Financial fraud, Etc.
Interrupted revenue, Forensic costs, Replacement costs, Incident mgmt person-hours, Etc.
Fines and judgements, Notification costs, Legal fees, Customer churn, PR costs, Etc.
Loss Event Scenario Chain of Events
Threats
Affect
Assets
Resulting in…
Loss Events
That have…
Primary Losses
And potentially…
Secondary Losses
Loss Event Prevention
Loss Magnitude Mitigation
Control Functions
Avoidance
Deterrence
Resistance
Detection
Visibility
Monitoring
Recognition
Response
Event Termination
Resilience
Loss Reduction
Example Controls
Network segmentation, IP address filtering, Hiring practices, Personnel mgmt, 3rd party due diligence, Etc.
Laws and policies, Logging and monitoring, Legal contracts, HR actions, Etc.
Authentication, Access privileges, Configuration settings, Anti-malware, Etc.
Logging, Cameras, Etc.
SIEM, Log reviews, Etc.
AV signatures, Checksums, Admin account inventories, Etc.
Forensics, Incident response, Etc.
Recovery processes, Data backups, Etc.
Legal actions, Credit monitoring, Insurance, Etc.

3.1 | Loss Event Prevention



3.1.1 | Avoidance

"Reduce the frequency of contact between threat agents and the assets they could adversely affect."

Before a loss event can occur, a threat agent has to come into contact with an asset that could be negatively affected. Contact may be physical or virtual (e.g., over a network). Also, threat agents can be humans, other animals, acts of nature, or even technologies, and they may or may not be malicious. For example, employees can inadvertently cause harm by accidentally damaging a facility, equipment, data, or other people. Similarly, Mother Nature can cause harm through weather events, earthquakes, and fires. Consequently, we can reduce the probability of some types of loss events by limiting contact between threat agents and the assets we are protecting.

Note that in some cases, Avoidance controls aren't a realistic option. For example, assets whose value is dependent upon being easily accessible (e.g., retail websites) may have few, if any, control opportunities for limiting contact with cybercriminals.

In environments where multiple layers of defense exist, defenses on outer layers can be considered Avoidance controls for inner layers. For example, anti-malware protection at the network perimeter can be viewed as an Avoidance control for assets inside the perimeter, as the outer layers reduce the probability that malware can reach assets on the inner layers.

Relationships and Dependencies

The Avoidance function has a Boolean OR relationship with the Deterrence and Resistance functions. In other words, if controls serving any of these functions are in place and operating as intended, the probability of a loss event occurring is reduced accordingly. If multiple controls serving any of these functions are in place and operating as intended, then the effect of these controls is cumulative.

Example Controls

- Network firewalls that block network access to systems and applications.
- IP address filtering at a network boundary that blocks network access from unauthorized sources.
- Hiring practices that reduce the probability of hiring criminals who may act maliciously or persons who are unqualified and may cause harm unintentionally.
- Security gates or fences that reduce the probability of illicit entry into facilities.
- Geographic positioning that reduces the probability of experiencing certain types of weather or geological events.

Unit of Measurement:

% reduction in contact frequency with threat agents

3.1.2 | Deterrence

"Reduce the probability of potentially harmful actions after a threat agent has come into contact with an asset."

Discussion

Once a potential threat has come into contact with an asset, there may be opportunities to affect the probability that it will act in a manner that could negatively impact the asset. Typically, these controls are thought of as only applying to scenarios where the threat is malicious, but Deterrent controls can also be helpful in non-malicious scenarios (e.g., campground signs regarding campfire restrictions). When threat agents are not cognitive (e.g., weather events), Deterrence controls are not relevant.

Regardless of whether a threat is malicious or not, Deterrence controls typically affect a threat's decision-making in one or more of the following ways:

- Reducing the perceived value of their actions (e.g., obscuring the value of an asset)
- Increasing the perceived difficulty/cost of acting (e.g., hardening the defenses surrounding an asset), or
- Increasing the threat's perception of risk to themselves from performing a harmful act (e.g., increasing the odds of getting caught and/or the consequences of being caught)

It's important to note that the efficacy of Deterrence controls is unlikely to be 100% because extreme behaviors are always possible. That said, Deterrence controls can significantly reduce the probability of threat actions in some circumstances.

Relationships and Dependencies

The Deterrence function has a Boolean OR relationship with the Avoidance and Resistance functions. In other words, if controls serving any one of these functions are in place and operating as intended, the probability of a loss event occurring is reduced accordingly. If multiple controls serving any of these functions are in place and operating as intended, then the effect of these controls is cumulative.

Example Controls

- Laws and legal notices
- Monitoring
- Enforcement of policies
- Obfuscation of asset value

- Hardened assets

Unit of Measurement

% reduction in the probability that threat actors would choose to act in a way that could result in harm

3.1.3 | Resistance

Function Description

"Reduce the likelihood that a threat agent's action(s) will result in a loss event."

Discussion

When a threat acts in a manner that could result in harm, there may be controls that reduce the probability that harm materializes. Common examples in malicious scenarios are passwords, privilege restrictions, and encryption, which a malicious actor must overcome or bypass to achieve their objectives.

However, although Resistance controls commonly apply to scenarios where threats are malicious, they also can apply to non-malicious scenarios. For example, a new software release could have coding errors that result in outages or computational errors, which would constitute a loss event. In this scenario, the developers are potential threat agents who are necessarily in contact with the software (so Avoidance controls are not applicable), and their purpose is to develop and release the code (so Deterrence controls are only appropriate if their intent is malicious). In this scenario, Resistance controls would be anything (e.g., pre-production testing, etc.) that reduces the probability that a software release directly results in loss events.

Relationships and Dependencies

The Resistance function has a Boolean OR relationship with the Avoidance and Deterrence functions. In other words, if controls serving any one of these functions are in place and operating as intended, the probability of a loss event occurring is reduced accordingly. If multiple controls serving any of these functions are in place and operating as intended, then the effect of these controls is cumulative.

Example Controls

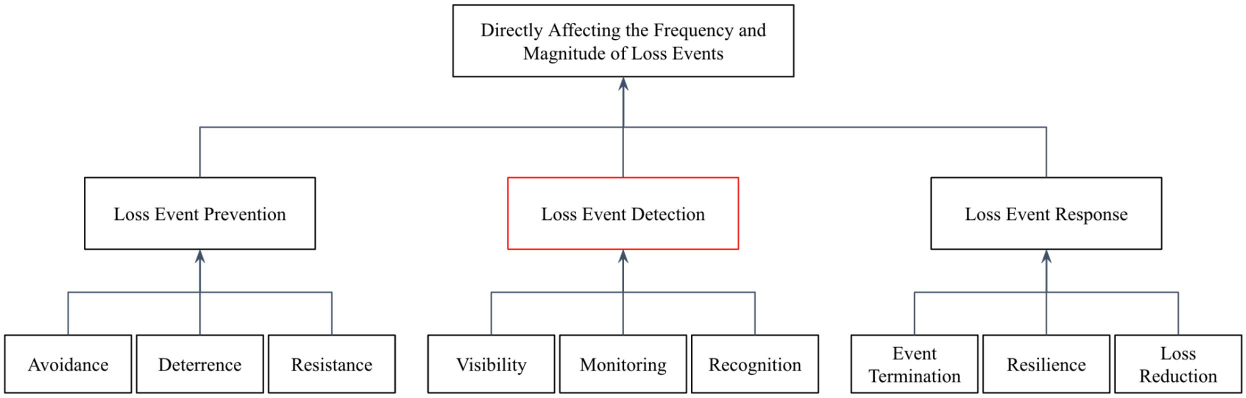
- Authentication mechanisms
- Privilege restrictions
- Software or systems without exploitable weaknesses
- Encryption

- Employees capable of recognizing social engineering attempts

Unit of Measurement

% probability of resisting potentially harmful actions by threat actors

3.2 | Loss Event Detection



It’s intuitive to understand that you must recognize something is amiss before you can react to it. This fact captures the Boolean AND relationship between Loss Event Detection and Loss Event Response. However, measuring the efficacy of Loss Event Detection requires us to understand and independently measure the various sub-functions that enable Detection.

It’s helpful to note that, at least in the cybersecurity context, many Detection control technologies provide visibility, monitoring, and recognition in one package. For example, anti-malware technologies capture activity on systems and/or networks (providing Visibility), evaluate the captured data (providing Monitoring), and have heuristic and signature databases with which to recognize malicious code (providing Recognition). However, this multi-function capability is not exclusive to cybersecurity, as guard dogs fulfill similar Visibility, Monitoring, and Response functions (as well as Deterrence and even Resistance) in physical security scenarios.

3.2.1 | Visibility

Function Description

“Provide evidence of activity that may be anomalous or illicit.”

Discussion

In order to detect that a loss event has occurred or is in progress, there has to be data that provides evidence of what has transpired. In scenarios involving physical threats, data might take the form of closed-circuit television cameras. In scenarios involving technology, data usually comes in the form of logging.

Note that visibility measurement tends to be strongly affected by the scope of an analysis. For example, an organization can say that cameras covering a specific facility entrance provide 100%

visibility into events transpiring at that entrance. But if that's one of four entrances to a facility, their overall visibility for entrances to that facility is only 25%. Similarly, in a cybersecurity context, an organization can claim to have 100% visibility for a specific form of attack (e.g., SQL injection) against a particular web application, but if that's the only web application that has logging turned on, then overall visibility will be less.

This scope-related dependency means there has to be clarity on the threats, forms of attack, and assets at risk in order to ensure measurement accuracy.

Relationships and Dependencies

The Visibility function has a Boolean AND relationship with the Monitoring and Recognition functions. In other words, if controls serving any of these functions are sufficiently deficient, detection won't occur, and the organization cannot mount a timely response.

Example Controls

- System, network, or application logs
- CCTV cameras
- Audio sensors
- Guard towers
- Anti-malware technologies
- Guard dogs

Unit of Measurement

% probability that the control provides access to the necessary information

3.2.2 | Monitoring

Function Description

“Review data provided by Visibility controls.”

Discussion

If data exists that provides evidence of potential loss events, then for that data to be useful, someone or something has to examine the data in order for detection to occur.

It is important to note that the unit of measurement for monitoring is time — i.e., how much time expires between reviews. Analytically, this is important because loss event scenarios have a “velocity” dimension, defined as how long it takes an event to go from the first moment after the loss event occurs to when the event results in maximum loss. If a loss event’s velocity is in days, but monitoring takes place every hour, then the opportunity to contain, recover, and minimize loss is much greater than if a loss event’s velocity is in hours but monitoring takes place every few days.

Relationships and Dependencies

The Monitoring function has a Boolean AND relationship with the Visibility and Recognition functions. In other words, if controls serving any of these functions are sufficiently deficient, detection won’t occur, and the organization cannot mount a timely response.

Example Controls

- Personnel reviewing logs manually
- SIEM systems
- IDS and IPS technologies
- Anti-malware technologies
- Guard dogs

Unit of Measurement

Elapsed time between reviews

3.2.3 | Recognition

Function Description

Enable differentiation of normal activity/conditions from abnormal activity/conditions that may indicate a loss event has occurred or is in progress.

Discussion

Recognition controls aim to distinguish normal, legitimate activity, conditions, and actors from abnormal and potentially harmful ones. It's important to note that some conditions and activities are obviously harmful, while others may only be distinguishable against established baselines. For example, a brute force password attack against a website is likely to be easily recognizable as malicious (unless it's an approved test of the system), yet a remote log-in from another country might only be suspected to be cause for alarm if it happens after hours and has never happened before.

This distinction between obvious vs. un-obvious activity/conditions means that Recognition control efficacy is often sensitive to the scope of an analysis (e.g., the type of threat action, who or what the threat is, etc.).

Relationships and Dependencies

The Recognition function has a Boolean AND relationship with the Visibility and Monitoring functions. In other words, if controls serving any of these functions are sufficiently deficient, detection won't occur, and the organization cannot mount a timely response.

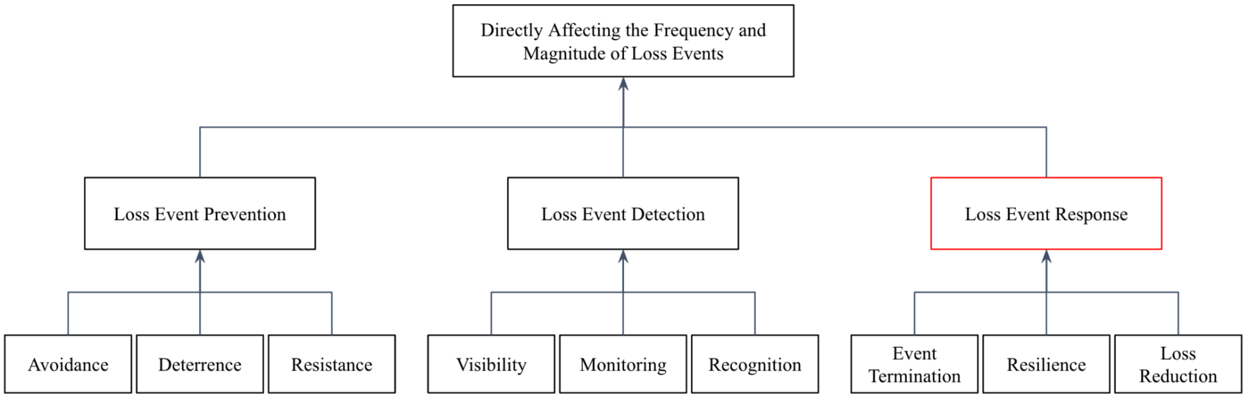
Example Controls

- Checksums
- Baseline activity records
- Time signatures
- Malware signatures
- Guard dogs

Unit of Measurement

% probability that a loss event will be successfully differentiated from normal activities or conditions.

3.3 | Loss Event Response



These controls come into play once a loss event has been recognized as having occurred. As was mentioned in the Loss Event Detection section, Loss Event Response has a Boolean AND dependency on Loss Event Detection — i.e., you can't respond to an event you aren't aware of.

The point of Loss Event Response is to the harm that materializes from loss events.

3.3.1 | Event Termination

Function Description

> ***"Enable termination of threat agent activities that could continue to be harmful."***

Discussion

Most loss events transpire over a period of time as opposed to taking place in the span of a moment. For example, a cybercriminal who gains a foothold on someone's corporate laptop takes time to find and exploit additional systems and information. Similarly, the longer flood water persists in a basement or warehouse, the more damage occurs. Consequently, limiting the time a threat can persist in an environment can significantly affect the amount of loss that materializes.

Note that, similar to the Monitoring control function, the unit of measurement for Event Termination is time, which means that its efficacy is also relative to a loss event's velocity.

Relationships and Dependencies

Event Termination has a "weak" Boolean AND relationship with Resilience and Loss Reduction. In other words, deficiencies in one of these sub-functions will diminish overall Response efficacy but won't necessarily inhibit it entirely.

Example Controls

- Incident response process
- Forensics
- Restoring known-good versions of software
- Segregating affected assets
- Termination of threat agents or termination of their access to the asset(s) at risk

Unit of Measurement

The amount of time that expires between recognition that a loss event has occurred and the point at which control over the event has been achieved.

3.3.2 | Resilience

Function Description

"Maintain or restore normal operations."

Discussion

Resilience controls aim to minimize the effect on operations from outage or degradation scenarios. For example, if a manufacturing production line is taken down by a power outage to the facility, backup electrical generators that support everyday operations or alternative connections to the power grid will reduce downtime.

Relationships and Dependencies

Resilience has a "weak" Boolean AND relationship with Event Termination and Loss Reduction. In other words, deficiencies in one of these sub-functions will diminish overall Response efficacy but won't necessarily inhibit it entirely.

Example Controls

- Backup and recovery processes
- Hot failover technologies
- Geographically distributed facilities
- VPN technologies that enable working remotely

Unit of Measurement

The amount of time operating in a degraded mode.

3.3.3 | Loss Reduction

Function Description

"Reduce the amount of realized losses from an event."

Discussion

When loss events occur, there sometimes are opportunities to limit the effect on an organization's bottom line or mission objectives. This outcome may be achieved by sharing loss exposure with insurers, recovering losses through legal actions, reducing customer churn, etc.

Relationships and Dependencies

Loss Reduction has a "weak" Boolean AND relationship with Event Termination and Resilience. In other words, deficiencies in one of these sub-functions will diminish overall Response efficacy but won't necessarily inhibit it entirely.

Example Controls

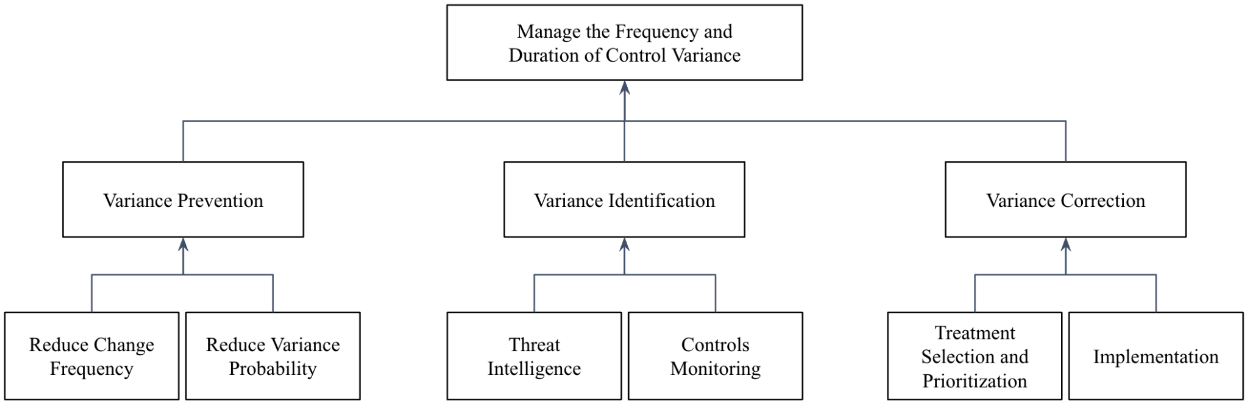
- Insurance
- Legal actions
- Resilience controls that support limited operations
- Transaction roll-backs
- Credit monitoring

Unit of Measurement

Reduction of lost economic value (e.g., dollars, Euros, etc.).

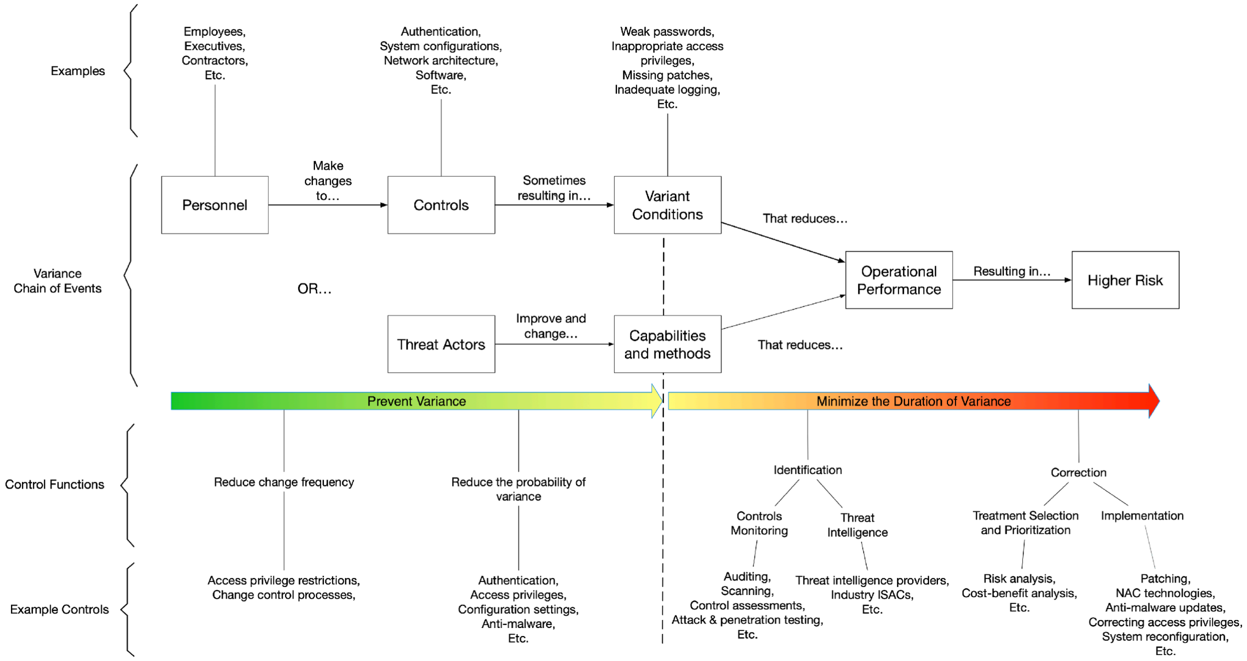
4 | The Variance Management Control (VMC) Functional Domain

Variance Management Controls affect the Operational Performance of other controls by limiting the frequency and duration of ineffective control conditions (i.e., variances from an intended state of efficacy).



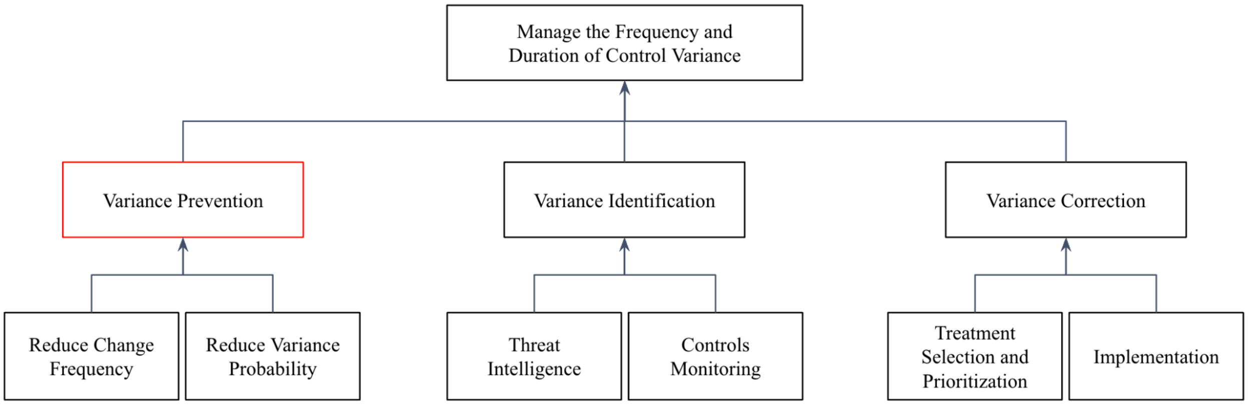
It is worth noting that Variance Identification and Variance Correction have a Boolean AND relationship to one another — i.e., both must exist in order to mitigate the effects of a loss event.

The diagram below illustrates how these control functions affect risk and provides some examples of controls that perform those functions.


Examples
Employees, Executives, Contractors, Etc.
Authentication, System configurations, Network architecture, Software, Etc.
Weak passwords, Inappropriate access privileges, Missing patches, Inadequate logging, Etc.
Variance Chain of Events
Personnel
Make changes to...
Controls
Sometimes resulting in...
Variant Conditions
That reduces...
Operational Performance
Resulting in...
Higher Risk
OR...
Threat Actors
Improve and change...
Capabilities and methods
That reduces...
Prevent Variance
Minimize the Duration of Variance
Control Functions
Reduce change frequency
Reduce the probability of variance
Identification
Controls Monitoring
Threat Intelligence
Correction
Treatment Selection and Prioritization
Implementation
Example Controls
Access privilege restrictions, Change control processes,
Authentication, Access privileges, Configuration settings, Anti-malware, Etc.
Auditing, Scanning, Control assessments, Attack & penetration testing, Etc.
Threat intelligence providers, Industry ISACs, Etc.
Risk analysis, Cost-benefit analysis, Etc.
Patching, NAC technologies, Anti-malware updates, Correcting access privileges, System reconfiguration, Etc.

It is tempting to think of VMCs as only relevant to the Operational Performance of Loss Event Controls. Many VMCs affect the reliability of other VMCs or even Decision Support Controls (DSCs). For example, asset discovery technologies can affect the Operational Performance of controls that Provide Asset Data (a DSC function). Consequently, these technologies act as a Variance Management Control (identifying and correcting variance) for an asset database (a Decision Support Control).

4.1 | Variance Prevention



Because operations-related variances (e.g., misconfigurations, etc.) typically occur when changes to a control or asset take place, it is possible to reduce these variances by either reducing the frequency of changes or by reducing the probability that variance will occur when a change occurs.

For example, new software releases always introduce the potential for a variant condition to be introduced to a platform or application. Therefore, it is possible to reduce the frequency of variance in these platforms or applications by either reducing the frequency of new releases or by instituting practices that reduce the probability that a new release will introduce a variant condition.

Another source of changes in control efficacy is threat-related — i.e., when new threats or threat capabilities come into existence that render existing controls ineffective (e.g., zero-day exploits). This source of variance is often outside of our control to prevent, yet still needs to be identified and remedied when it occurs.

4.1.1 | Reduce Change Frequency

Function Description

"Reduce the frequency of changes."

Discussion

Most variant conditions occur when a change occurs to a control or asset. Common examples include:

- New software releases
- Users installing unauthorized software on their personal devices
- Users changing their passwords
- Personnel changing roles or leaving an organization
- The addition of new technologies
- Creating new network connections
- Hiring new personnel

Note that the frequency of some changes may not be easily reduced, in which case the focus needs to be on reducing the probability that the change introduces some form of variant condition (which is the following control function in the model).

Relationships and Dependencies

Reducing Change Frequency has a Boolean OR relationship with Reducing Variance Probability based on the fact that reducing either will reduce the frequency of variance.

Example Controls

- Limit administrative privileges on personal devices (laptops, etc.)
- Limit superuser privileges on production systems
- Change control processes
- Reduce the frequency of software releases

Unit of Measurement

Forecast or measured % reduction in the frequency of changes that could introduce variance

4.1.2 | Reduce Variance Probability

Function Description

"Reduce the probability that changes will result in control degradation or failure."

Discussion

When changes occur to assets and controls, these changes sometimes degrade control performance — i.e., they introduce variance from an intended state of efficacy. Consequently, we apply controls that reduce the probability that when changes occur, variance will be introduced.

Most variant conditions occur because the person making the change either:

- Was unaware of what was expected
- Was incapable of complying with what was expected, or
- Chose not to comply

Regardless, in each case, the individual made a decision to perform the action they took, which is why many of the controls that support this function are Decision Support Controls (which are covered later in this document).

Note that because some variant conditions occur due to changes in the threat landscape, it is conceivable that an organization could reduce the probability of variant conditions by choosing controls or technologies that are not subject to frequent changes in the threat landscape. Although conceivable, this doesn't tend to be a commonly applied variance management strategy.

Relationships and Dependencies

Reduce Variance Probability has a Boolean OR relationship with Reduce Change Frequency because variance can be independently reduced with either one.

Example Controls

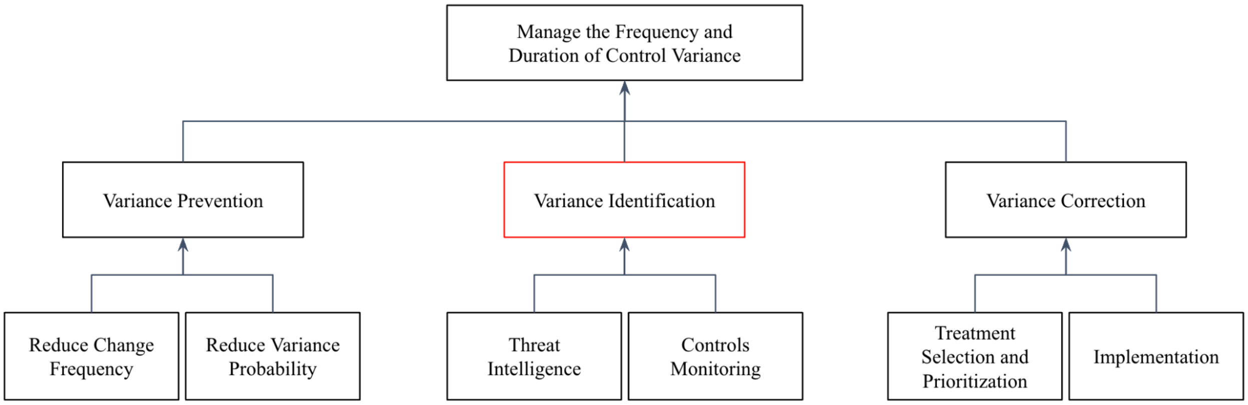
- Change review processes
- Allow/deny listing technologies
- Decision Support Controls
- Endpoint security enforcement technologies

- Pre-production application security testing

Unit of Measurement

Forecast or measured % reduction in variance

4.2 | Variance Identification



Because degradation in control performance (variances) can occur directly to controls themselves or indirectly through changes in the threat landscape, FAIR-CAM includes functions for identifying either source of variance. Inadequate visibility into these landscapes increases the persistence of variant conditions, resulting in longer exposure windows.

4.2.1 | Threat Intelligence

Function Description

"Identify changes in the threat landscape that diminish the efficacy of controls."

Discussion

The efficacy of controls sometimes diminishes due to changes in the threat landscape rather than changes to the controls themselves. As a result, it is important to be able to recognize when these changes occur so that adjustments to controls can be made. For example, cybercriminals may develop new exploits against a particular type of software, which renders previously secure applications vulnerable. Knowing about the new exploit makes it possible to fix the weakness or compensate for it in some other fashion.

The cybersecurity domain is not the only place where changes in the threat landscape occur. For example, changes in climate that produce more severe hurricanes may mean that levees no longer provide sufficient protection against storm surges. If we aren't aware of these climate changes, then we can't improve the associated controls.

Relationships and Dependencies

Threat Intelligence has a Boolean AND relationship with Variance Correction, given that you can't account for changes in the threat landscape that you aren't aware of.

Example Controls

- Cyber threat intelligence providers
- Cybersecurity information-sharing forums
- National intelligence agencies
- Climate monitoring
- Volcano monitoring

Unit of Measurement

Elapsed time between changes in the threat landscape and awareness of those changes.

4.2.2 | Control Monitoring

Function Description

"Identify variance in control conditions."

Discussion

Variant control conditions occur periodically, either intentionally or unintentionally. When they do, control efficacy is degraded and risk increases. Thus, Variance Management Controls that enable timely detection of these variant conditions should be employed.

Note that control monitoring frequency should be determined by how much additional risk exists when variance occurs. This is driven by several considerations, including:

- The value/liability of the assets at risk
- Threat event frequency

- How much a variant condition affects other controls
- Whether other compensating controls exist and are performing well

Relationships and Dependencies

Controls Monitoring has a Boolean AND relationship with Variance Correction, given that you can't correct variant conditions that you aren't aware of. Consequently, if either one is deficient, the duration of variant conditions will persist.

Example Controls

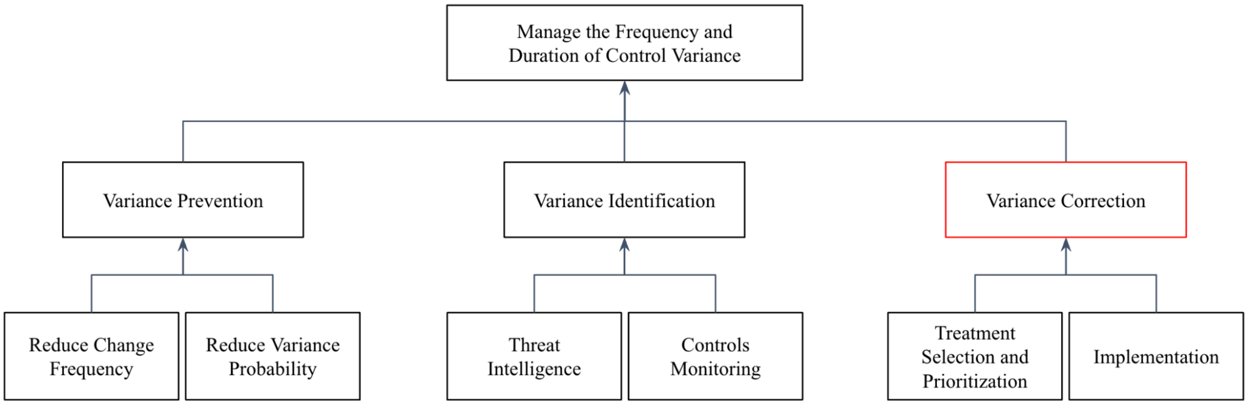
- Auditing
- Regulatory exams
- Vulnerability scanning
- Attack and penetration testing
- Configuration management tools

Unit of Measurement

Elapsed time between changes in control conditions and the recognition of those changes.

4.3 | Variance Correction

Variance Correction includes those controls that take place after variant conditions have been identified.



4.3.1 | Treatment Selection and Prioritization

Function Description

"Select and prioritize control variance corrections."

Discussion

Treatment Selection and Prioritization controls evaluate variant conditions and determine in what manner and how rapidly they should be corrected. Note that because selection and prioritization are instances of decision-making, this control function is primarily served by Decision Support Controls (e.g., risk analysis, cost-benefit analysis, etc.). If DSCs are missing or performing poorly, then inappropriate or ineffective treatments may be chosen, or the prioritization of treatments may be ill-timed.

Relationships and Dependencies

Boolean AND with Implementation

Example Controls

- Decision Support Controls (e.g., expectations, data, risk analysis, etc.)

Unit of Measurement

Elapsed time from the identification of a variant condition until corrective actions begin.

4.3.2 | Implementation

Function Description

"Correct variant conditions."

Discussion

When variant conditions have been identified and some form of correction is chosen and prioritized, the final step is the implementation of the correction.

Relationships and Dependencies

Boolean AND with Treatment Selection and Prioritization

Example Controls

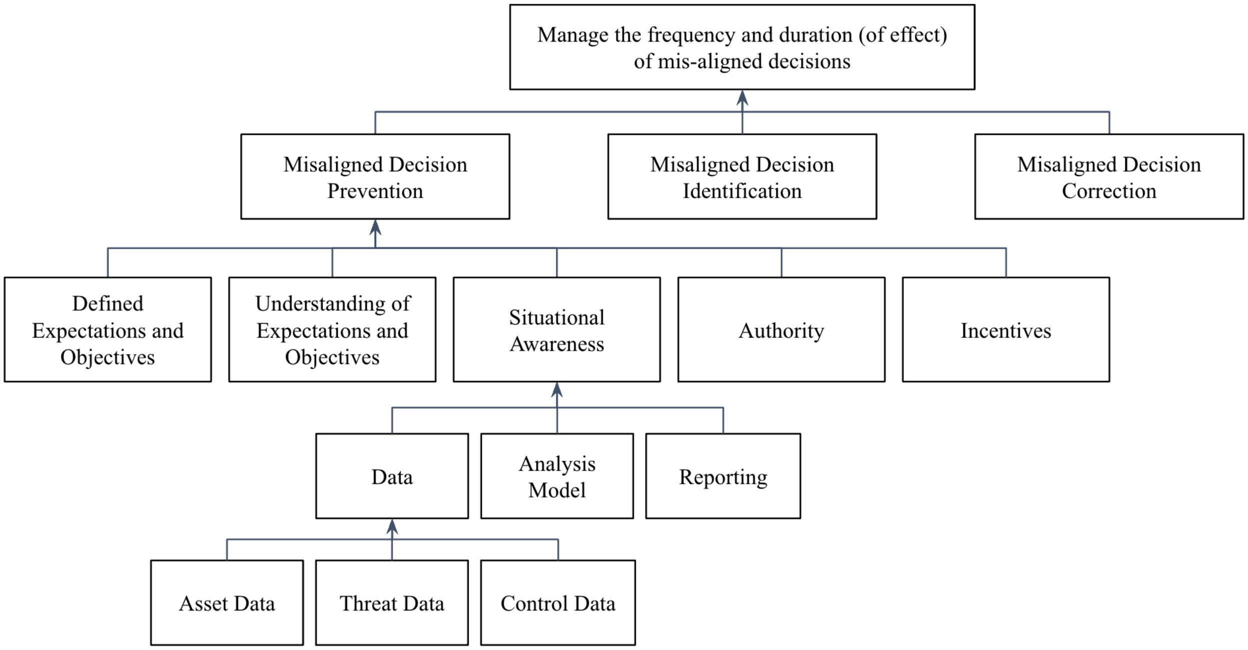
- Patching
- Reconfiguration of systems
- Process revisions
- Access privilege adjustments

Unit of Measurement

Elapsed time from initiation of corrective actions until their completion.

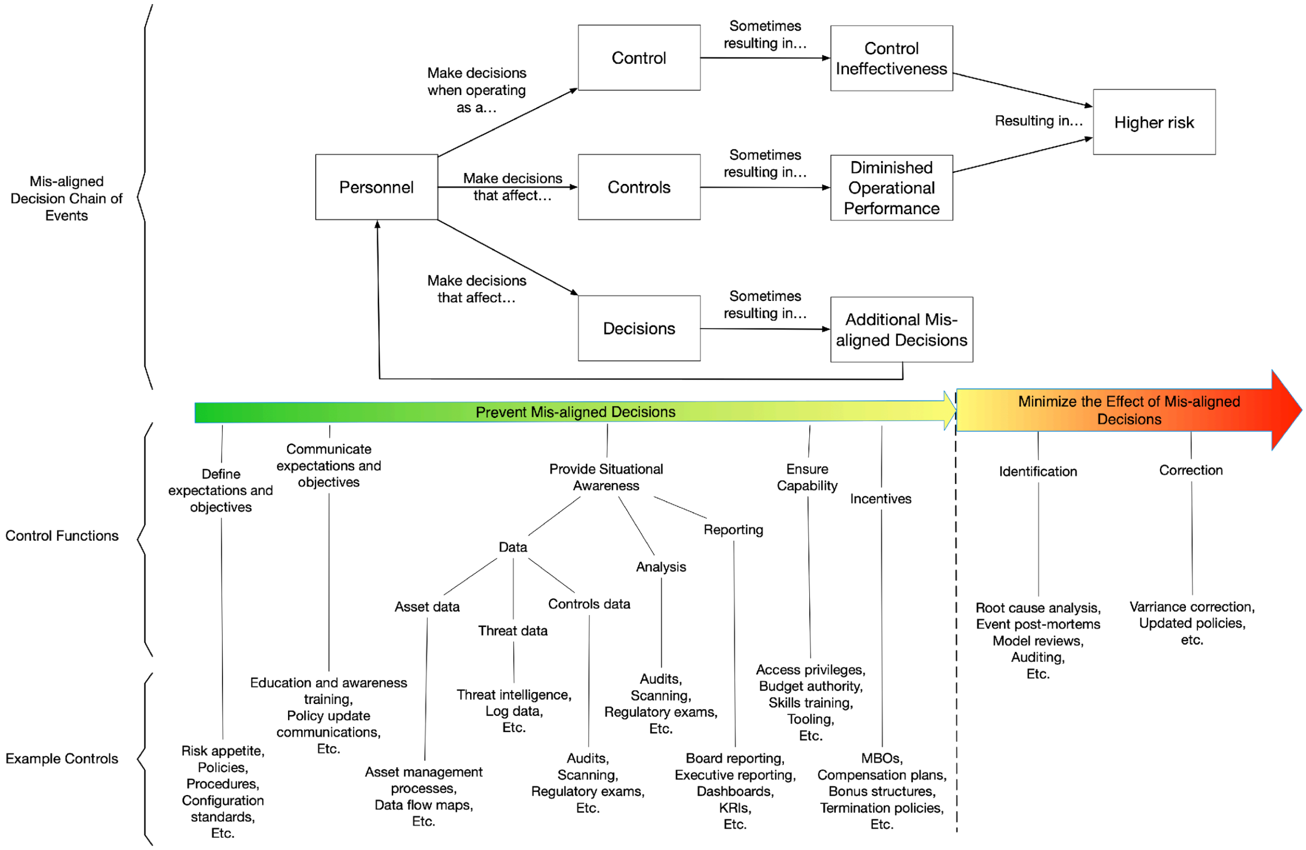
5 | The Decision Support Control (DSC) Functional Domain

Decision Support Controls help to ensure that decisions are aligned with organizational objectives and expectations.


Manage the frequency and duration (of effect) of mis-aligned decisions
Misaligned Decision Prevention
Misaligned Decision Identification
Misaligned Decision Correction
Defined Expectations and Objectives
Understanding of Expectations and Objectives
Situational Awareness
Authority
Incentives
Data
Analysis Model
Reporting
Asset Data
Threat Data
Control Data

It is worth noting that Misaligned Decision Identification and Misaligned Decision Correction have a Boolean AND relationship to one another — i.e., both must exist in order to mitigate the risk of poor decisions.

The diagram below illustrates how these control functions affect risk and provides some examples of controls that perform those functions.


Mis-aligned Decision Chain of Events
Personnel
Make decisions when operating as a…
Make decisions that affect…
Make decisions that affect…
Control
Controls
Decisions
Sometimes resulting in…
Sometimes resulting in…
Sometimes resulting in…
Control Ineffectiveness
Diminished Operational Performance
Additional Mis-aligned Decisions
Resulting in…
Higher risk
Prevent Mis-aligned Decisions
Minimize the Effect of Mis-aligned Decisions
Control Functions
Define expectations and objectives
Communicate expectations and objectives
Provide Situational Awareness
Data
Asset data
Threat data
Controls data
Analysis
Reporting
Ensure Capability
Incentives
Identification
Correction
Example Controls
Risk appetite, Policies, Procedures, Configuration standards, Etc.
Education and awareness training, Policy update communications, Etc.
Asset management processes, Data flow maps, Etc.
Threat intelligence, Log data, Etc.
Audits, Scanning, Regulatory exams, Etc.
Audits, Scanning, Regulatory exams, Etc.
Board reporting, Executive reporting, Dashboards, KRIs, Etc.
Access privileges, Budget authority, Skills training, Tooling, Etc.
MBOs, Compensation plans, Bonus structures, Termination policies, Etc.
Root cause analysis, Event post-mortems Model reviews, Auditing, Etc.
Varriance correction, Updated policies, etc.

This section of FAIR-CAM will include more explanation than the previous sections because decision alignment has historically received less explicit focus than other parts of the controls landscape.

The underlying context for DSCs is an assumption that organizations want to cost-effectively achieve and maintain an acceptable level of risk. The "cost-effective" component of this objective speaks to the fact that organizations have limited resources. The "acceptable level of risk" component of this objective accounts for the fact that there is always some level of risk an organization must accept in order to achieve its financial or mission objectives, yet having too much risk must also be avoided.

These cost management and risk considerations provide the context for determining whether risk management decisions are well aligned with an organization's objectives. In other words, if a decision results in levels of risk that exceed an organization's risk appetite or that drive risk levels unreasonably low, then the decision isn't well-aligned. Similarly, if a decision results in inefficient use of risk management resources, then it isn't well-aligned with the cost-efficiency objective.

Rather than starting with a detailed discussion of the functions within this domain, we'll begin by relating it to a couple of familiar decision-making scenarios. These won't represent comprehensive examples of how to apply the model, as a more comprehensive description will be provided in the *Applying the FAIR Controls Analytics Model* document. They are simply intended to make it easier to understand where DSCs fit into the picture, as well as the different ways in which they can affect risk.

Scenario 1 — DSC's role in Managing control variance

Imagine that audits within an organization frequently discover access privileges are not reliably updated when personnel leave the organization or change roles. The problem exists in multiple parts of the organization rather than within just one or two departments.

These inappropriate access privileges represent Resistive control variances — i.e., the Operational Performance of access privileges as a Resistive control is reduced. The more frequently this occurs and the longer these variances persist, the greater the potential for loss to occur.

In addition, the fact that this problem is relatively widespread and recurring has given auditors (both internal and external) concerns regarding whether the risk management program as a whole may be problematic, which has increased the depth and frequency of their audits. Supporting these audits has placed an additional load on already limited organization resources.

Using the DSC model as a diagnostic tool, we can perform a root cause analysis to better understand and address the problem:

- Have clear expectations been defined regarding the requirement to update access privileges when personnel leave the organization or change roles?
- Have those expectations been communicated to management personnel who are responsible for initiating the update process?
- Have management personnel been made aware of the risk implications associated with inappropriate access privileges (i.e., do they have reasonable situational awareness)?
- Do management personnel have the skills, technologies, and processes necessary to fulfill their access privilege responsibilities (i.e., are they capable)?
- Do effective incentives exist to motivate management personnel to fulfill their access privilege responsibilities?

In our hypothetical organization, let's assume that the answers to the first four bullets are "yes."

- A clearly defined policy exists regarding the need to update access privileges.

- Management personnel have all been given annual awareness training, which includes a section on access privilege management expectations.
- Included in the awareness training is information related to the importance of access privileges as a risk reduction measure, and management is inherently aware when personnel leave or change roles.
- A well-defined process has been established for initiating updates to access privileges, and a reasonably simple web app exists to support this purpose.

However, there are no clearly defined or enforced incentives to motivate compliance — i.e., there is no meaningful upside for compliance or downside for non-compliance. Management personnel are formally incentivized to meet revenue goals and cost management objectives, but they are not formally incentivized to fulfill their access privilege management responsibilities. Adding and enforcing explicit access management objectives to their MBOs (an Incentive Control) is likely to affect the decision-making of management personnel, reducing the frequency of decisions that are misaligned with the organization's objectives and decreasing the frequency of access privilege variance, which ultimately decreases risk. It also may eventually help to reduce the costs incurred by more invasive and more frequent auditing.

Scenario 2 — DSC's role in control choices

An organization is considering whether or not it should upgrade its multi-factor authentication (MFA) solution. The current solution has been effective as a Resistive control for several years, but the threat landscape continues to evolve in ways that have reduced its efficacy. Consequently, a proposal has been put forth to upgrade the organization's MFA solution.

In this scenario, we'll assume the organization has clearly defined objectives with regard to the efficacy of an MFA solution and that the decision-makers know what those expectations are. The Data, Analysis, and Reporting functions within Situational Awareness provide decision-makers with information regarding current risk levels, as well as how those risk levels are likely to change with various MFA solutions. Assuming that results from the Situational Awareness controls indicate an MFA upgrade is warranted, the organization will also need to ensure that it has the necessary capabilities in terms of skills and resources to support making a change.

Last but not least, in order to maximize the odds of the decision being aligned with the organization's broader objectives, incentives need to be in place that help decision-makers make appropriate trade-offs between the risk management goals, revenue or mission-related goals, and cost containment goals. For example, if the decision-maker is heavily incentivized to contain costs but isn't incentivized to meet risk management objectives, there's a greater likelihood they will decide not to upgrade MFA despite risk analysis results that indicate an upgrade is appropriate.

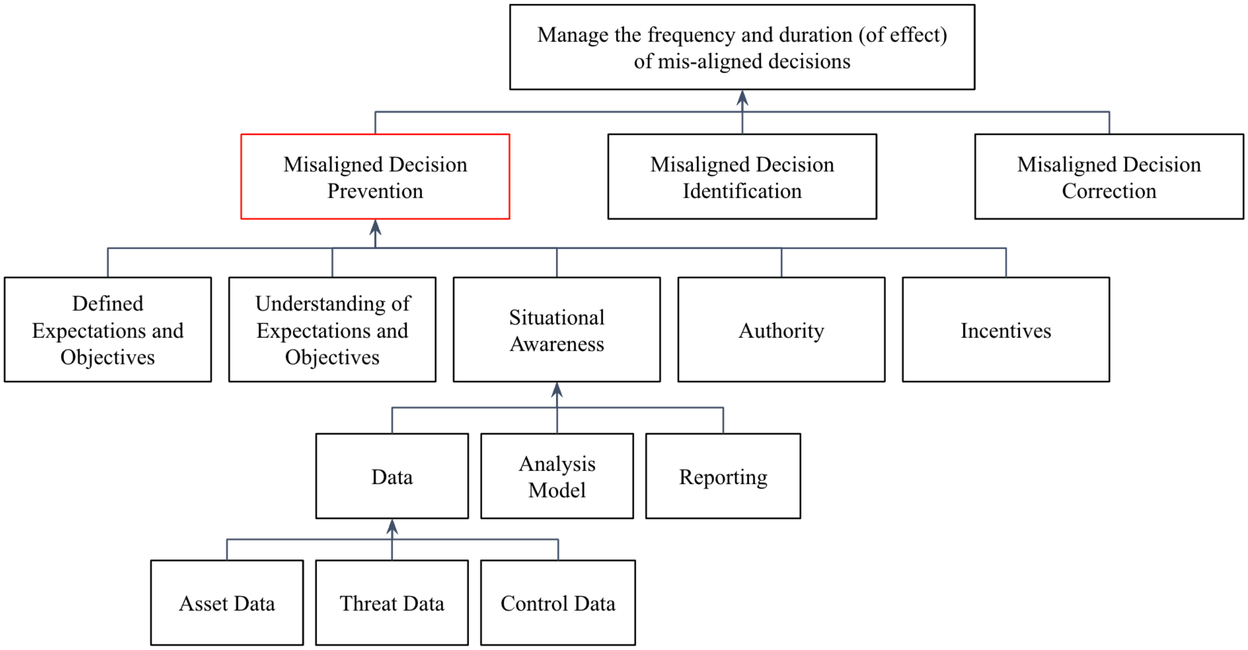
A couple of things worth highlighting in this scenario are:

- If clear expectations have not been defined or communicated regarding MFA efficacy, then Situational Awareness results will be open to interpretation. For example, if the organization (or a regulating agency) has simply established an expectation that “MFA must be used” (a box-checking compliance requirement), then any risk reduction from a MFA product upgrade will be less relevant to decision-makers.
- If the Data or Analysis functions within Situational Awareness are especially poor or inherently flawed, then it’s more likely that a poor decision will be made. For example, if the risk analysis is reliant upon an analyst’s mental model versus a risk model that has been vetted, there’s a greater opportunity for analytic errors or bias in the results. If error or bias results in a decision to upgrade MFA when it isn’t necessary, then the organization is inefficient in its use of limited resources. Those wasted resources won’t be available for other, more important risk management efforts or other organization imperatives. Conversely, if poor Situational Awareness results in an errant decision to not upgrade, then the organization is unknowingly taking on more risk than it should.

Scenario wrap-up

Hopefully, these two scenarios will make the following descriptions easier to understand and apply. As was mentioned earlier, the “Applying the FAIR Controls Analytics Model” document will provide many more examples and additional information regarding how to leverage the DSC component of FAIR-CAM.

5.1 | Preventing Misaligned Decisions


Manage the frequency and duration (of effect) of mis-aligned decisions
Misaligned Decision Prevention
Misaligned Decision Identification
Misaligned Decision Correction
Defined Expectations and Objectives
Understanding of Expectations and Objectives
Situational Awareness
Authority
Incentives
Data
Analysis Model
Reporting
Asset Data
Threat Data
Control Data

It's one thing to define and measure control specifications for a piece of technology or a business process. It's another thing to define and measure the effect of controls on human decision-making. Note that FAIR-CAM does not delve into psychometrics or try to gauge the rationality or judgment of decision-makers. Instead, it focuses on control functions that improve the odds of decisions being well-aligned with organizational objectives.

It should be pointed out that weaknesses in these control functions can be compensated for to some degree by the experience, intelligence, judgment, and ethics of decision-makers. Unfortunately, these traits can be highly variable within a population of personnel. Consequently, the more diligently an organization approaches Decision Support Controls, the more effective its risk management program will be, and the greater the likelihood that its objectives will be achieved.

It is also important to remember that decisions occur at all levels within an organization:

- Executives make decisions about objectives, policies, budget allocations, and strategies
- Management makes decisions about operational priorities, specific solutions, and resource allocations, and

- Personnel at all levels make decisions regarding their individual actions (e.g., use of organization resources, communication of organization information, password choices, system & network administration, etc.)

The fact that these decisions are being made every day means that systemic weaknesses in decision-making can be crippling. However, even non-systemic weaknesses in decision-making can materially increase the odds of significant losses and missed objectives.

5.1.1 | Defined Expectations

Function Description

"Clearly define expectations and/or objectives."

Discussion

Absent clearly defined expectations and objectives, decision-makers are left to their own biases and judgments regarding where the goal lines are and what the priorities should be. When this happens, there is a greater probability for decisions to expose an organization to excessive risk and wasted resources. Conversely, when expectations and objectives are more specific and clearly defined, the probability increases that decisions will support those goals.

For example, the risk appetite statement "The organization has a low appetite for risk" is limited in its ability to support well-aligned decision-making. The word "Low" is simply too ambiguous and open to interpretation. If, instead, an organization defines specific thresholds for risk, in the form of measures of loss exposure, probability of mission failure, KRI thresholds, etc., then decision-makers are better able to calibrate their decisions. It also makes it much easier to hold decision-makers accountable.

Similarly, objectives such as "Network Integrity is Protected" can mean different things to different people. Some decision-makers may leverage the ambiguity in that objective to simply check compliance-related boxes, while other decision-makers may leverage the ambiguity to fight for excessive levels of control. In either case, the objectives of the organization are not well served.

Relationships and Dependencies

This has a Boolean AND relationship with the other DSC/Prevention control functions — i.e., even if the other functions are operating well, deficiencies in this function will increase the probability of misaligned decisions.

Example Controls

- Risk appetite definition
- Policies
- Process definitions
- Configuration standards
- Regulatory requirements
- Risk acceptance authority levels
- KRI & KPI thresholds

Unit of Measurement

The probability that clear expectations and objectives have been defined.

5.1.2 | Communication of Expectations

Function Description

"Communicate expectations to responsible personnel."

Discussion

Well-defined expectations and objectives are of little decision-making value if decision-makers aren't aware of them. With this in mind, many organizations have implemented formal risk management education and awareness programs. Unfortunately, many of those programs are relatively superficial and generic in nature, limiting the covered topics to things like anti-phishing, choosing strong passwords, etc.

Although these more generic topics are important, many personnel groups also have very specific risk-related responsibilities, which also need to be well communicated. For example, relatively few organizations have specific awareness programs for system and network administrators. Instead, there's an assumption that they are aware of what's expected of them from a risk management perspective. Similarly, executive administrative assistants rarely receive specific awareness training related to handling their risk-related responsibilities.

By providing more specific awareness training to specific audiences, an organization not only increases the level of awareness for those personnel but also emphasizes the importance and accountability of their decisions.

Relationships and Dependencies

This has a Boolean AND relationship with the other DSC/Prevention control functions — i.e., even if the other functions are operating well, deficiencies in this function will increase the probability of misaligned decisions.

Example Controls

- Education & awareness training
- Performance requirements
- Online policy websites
- Policy update notices

Unit of Measurement

The probability that expectations and objectives have been clearly communicated to decision-makers.

5.1.3 | Provide Situational Awareness

The purpose of Situational Awareness is to provide decision-makers with an understanding of not only the current risk landscape conditions but also the potential implications of their decisions. Note that the quality of Situational Awareness is based upon a set of sub-functions (Data, Analysis, and Reporting) and the controls that support those sub-functions.

5.1.3.1 | Provide Data

The Data function provides information that feeds the analysis and reporting functions within Situational Awareness. Note that the quality of the Data function is based upon a set of sub-functions (Asset data, Threat data, and Controls data) and the controls that support those sub-functions.

5.1.3.1.1 | Provide Asset Data

Function Description

“Provide data regarding the assets that are relevant to or affected by decisions.”

Discussion

Controls serving this function help to ensure that organizations are aware of the existence and value/liability characteristics of the assets they rely on. This information helps organizations understand the loss implications of the assets and, thus, which assets warrant greater/lesser protection.

Note that the "value" proposition of assets is from the asset owner's perspective (versus a threat agent's perspective). The "liability" proposition of assets is considered to be the potential harm that may occur from owning, using, losing, etc., the asset. Examples include the potential liability that comes from using volatile chemicals or from losing patient health information.

It also is important to note that "assets" are not simply cash, data, facilities, technologies, equipment, etc. Personnel, business processes, and relationships also are examples of assets. Essentially, anything that provides value or benefit toward the achievement of objectives can be considered an asset.

Relationships and Dependencies

This has a Boolean AND relationship with the other DSC/Prevention control functions — i.e., even if the other functions are operating well, deficiencies in this function will increase the probability of misaligned decisions.

Example Controls

- Asset management technologies
- Data Loss Prevention technologies
- Asset inventory processes
- Business process diagrams
- HR databases
- Accounting records

Unit of Measurement

Probability that asset data used to support a decision is accurate.

5.1.3.1.2 | Provide Threat Data

Function Description

"Provide data regarding relevant threats."

Discussion

In order to understand the types, frequency, and severity of loss events an organization faces, it is necessary to understand the threat landscape.

Note that a "threat" is anything that can act in a manner that results in harm. These may be humans, other animals, acts of nature, technology failures, or others. Threat actions may be intentional, accidental, incidental, or natural.

It's also important to note that some threats are more dynamic than others, and some have greater potential for material harm than others. Recognizing and accounting for this in their threat data solutions will help to ensure that organizations have higher quality threat data, which supports better risk-related decisions.

Relationships and Dependencies

This has a Boolean AND relationship with the other DSC/Prevention control functions — i.e., even if the other functions are operating well, deficiencies in this function will increase the probability of misaligned decisions.

Example Controls

- Network, system, application, firewall, etc., logs
- Seismic monitors
- Crime statistics from law enforcement agencies
- Threat intelligence providers
- Information sharing organizations
- Network service providers

Unit of Measurement

Probability that threat data used to support a decision is accurate.

5.1.3.1.3 | Provide Controls Data

Function Description

"Provide data regarding the condition of controls that are relevant to decisions."

Discussion

Controls serving this function provide information regarding the existence and condition of controls.

Because many controls serve multiple control function purposes (e.g., anti-malware solutions commonly fulfill Resistive, Visibility, Monitoring, Recognition, and Containment functions), it is valuable to identify which functions a control fulfills as well as its Operational Performance levels in serving those functions. This helps to ensure that the effect of those controls can be appropriately accounted for in risk and gap analyses.

Relationships and Dependencies

This has a Boolean AND relationship with the other DSC/Prevention control functions — i.e., even if the other functions are operating well, deficiencies in this function will increase the probability of misaligned decisions.

Example Controls

- Audits
- Training records
- Configuration management technologies
- Anti-malware technologies
- Vulnerability scanning
- Penetration testing
- Process reviews

Unit of Measurement

Probability that controls-related data used to support a decision is accurate.

5.1.3.2 | Analysis

Function Description

"Synthesize asset, threat, and controls data and generate accurate results."

Discussion

In complex problem spaces like cybersecurity and other risk disciplines, the ability to generate accurate results from data is crucial in order to avoid poor decisions. Historically, many risk management decisions have been based primarily upon either the uncalibrated mental models of professionals or models that are demonstrably flawed. As a result, organizations have struggled to accurately measure or cost-effectively manage risk.

For example, many organizations use CVSS (Common Vulnerability Scoring System) scores to prioritize their vulnerability management efforts. Unfortunately, CVSS scores are not a reliable indication of how much risk a vulnerability represents, as they do not take into account the level of threat activity an asset faces (Internet-facing vs. protected behind layers of defense), whether other compensating controls are in place, or (often) the value/liability proposition of the assets at risk. The result is that many organizations are unnecessarily aggressive in treating low-risk vulnerabilities that have high CVSS scores. This starves other, more important risk management efforts, places unwarranted pressure on personnel who are responsible for remedying vulnerabilities, and increases the risk associated with patches that introduce operational degradation or outages.

Relationships and Dependencies

This has a Boolean AND relationship with the other DSC/Prevention control functions — i.e., even if the other functions are operating well, deficiencies in this function will increase the probability of misaligned decisions.

Example Controls

- FAIR
- NIST 800-30
- Proprietary risk models
- Analyst mental models

NOTE: These are examples only. Inclusion in this list should not be considered an endorsement of efficacy. For example, NIST 800-30 table G5 has a known logical flaw that systematically inflates risk scoring.

Unit of Measurement

Probability that an analysis model will generate accurate results provided that it has accurate data.

- Backtesting against historical events
- Simulation environments (e.g., agent-based modeling)
- Detailed examination of model constructs (e.g., looking for logical errors, inappropriate use of data, etc.)

5.1.3.3 | Reporting

Function Description

"Provide decision-makers with analysis results."

Discussion

Some risk-related decisions are routine and planned for. However, the risk landscape tends to be highly dynamic, which means that many decisions must be made with less time for preparation. Regardless of whether decisions are routine or not, having updated situational awareness helps to ensure that decisions are aligned with the organization's objectives.

It is important to note however, that it isn't enough to simply provide information to decision-makers. The information also has to be relevant to the decision at hand, and it has to be understood by the decision-maker. Consequently, when measuring the efficacy of process and technology controls that fulfill this function, it's important to discount reporting that fails to fulfill these criteria.

Relationships and Dependencies

This has a Boolean AND relationship with the other DSC/Prevention control functions — i.e., even if the other functions are operating well, deficiencies in this function will increase the probability of misaligned decisions.

Example Controls

- Periodic reporting (weekly, monthly, quarterly, etc.)
- Dashboards
- Ad hoc reporting

Unit of Measurement

Probability that useful analysis results are provided to decision-makers in time to support their decisions.

5.1.4 | Ensure Capability

Function Description

“Ensure that the decision-maker has the necessary skills, authority, and resources to make decisions that are aligned with the organization’s expectations and objectives.”

Discussion

Decision-makers may know what’s expected of them, and they may have sufficient situational awareness to know what their decision should be, but if they lack the skills, authority, or resources to make a well-aligned decision, then they are more likely to make misaligned decisions.

For example, one organization had set and communicated an expectation that any email containing sensitive information had to be encrypted. Personnel also had sufficient situational awareness to recognize what constituted sensitive information. Unfortunately, personnel had not been provided training on how to use the new encryption feature of the organization’s email solution. Consequently, emails containing sensitive information continued to be sent unencrypted.

Relationships and Dependencies

This has a Boolean AND relationship with the other DSC/Prevention control functions — i.e., even if the other functions are operating well, deficiencies in this function will increase the probability of misaligned decisions.

Example Controls

- Budget authority
- Access privileges
- Skills training
- Tools and procedures
- Project management

Unit of Measurement

The probability that responsible persons will have the skills and resources necessary to act in a manner that is aligned with expectations.

5.1.5 | Incentives

Function Description

"Motivate personnel to make decisions that are aligned with the organization's expectations and objectives."

Discussion

Organizations commonly incentivize their risk management professionals to meet specific risk management objectives. However, few organizations formally incentivize personnel outside of the risk management departments to meet risk management objectives. This is problematic because every person within an organization has some level of risk management responsibility. In fact, many of these non-risk-department personnel have very significant and far-reaching risk management responsibilities, but they are only incentivized to meet the organization's mission, revenue, and cost containment objectives. As a result, when faced with fulfilling their risk management responsibilities versus mission/revenue/cost responsibilities, risk management often gets deprioritized.

Relationships and Dependencies

This has a Boolean AND relationship with the other DSC/Prevention control functions — i.e., even if the other functions are operating well, deficiencies in this function will increase the probability of misaligned decisions.

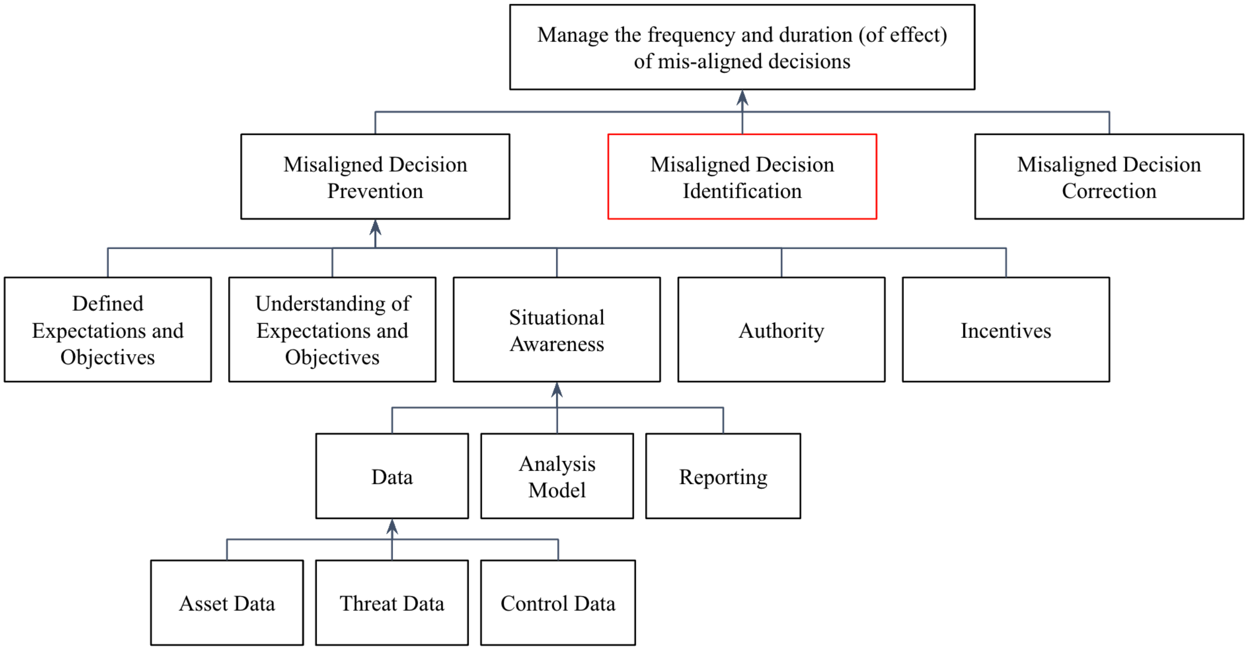
Example Controls

- MBOs
- Bonus criteria
- Laws and regulations
- Contract provisions
- Employment criteria

Unit of Measurement

The probability that appropriate incentives are in place to encourage well-aligned decisions.

5.2 | Identifying Misaligned Decisions


Manage the frequency and duration (of effect) of mis-aligned decisions
Misaligned Decision Prevention
Misaligned Decision Identification
Misaligned Decision Correction
Defined Expectations and Objectives
Understanding of Expectations and Objectives
Situational Awareness
Authority
Incentives
Data
Analysis Model
Reporting
Asset Data
Threat Data
Control Data

Function Description

> ***"Enable the identification of decisions that were not aligned with the expectations and objectives of the organization."***

Discussion

Regardless of how much effort goes into preventing them, some misaligned decisions inevitably will occur. And because these decisions can materially affect the odds of whether an organization is able to achieve its objectives, it's important to proactively search for misalignment — particularly signs of systemic misalignment.

In order to search for decision misalignment, we have to keep in mind where decisions occur, for example:

- Expectation setting (e.g., policies, processes, thresholds for action, etc.)
- Prioritization (e.g., resource allocations, etc.)
- Solution/remediation choices
- Compliance with expectations/performance of responsibilities

Another necessary component is clarity on what the organization's expectations/objectives are. Absent that clarity, it becomes much more difficult to confidently recognize misalignment when it occurs. For example, if there’s a lack of clarity regarding an organization’s risk appetite, then evaluating whether KRI thresholds are aligned with the organization’s risk appetite is more difficult.

Unfortunately, most organizations do not systemically or rigorously address this function. Postmortems and policy reviews may occur, but other key opportunities for fulfilling this function are not commonly employed. This is particularly true in regards to identifying systemic misalignments and their causes through root cause analysis. As a result, it is common to see organizations playing risk management “whack-a-mole,” fighting the same battles repeatedly.

Relationships and Dependencies

This has a Boolean AND relationship with the Defined Expectations function, which provides the baseline for comparing a current state versus a desired state.

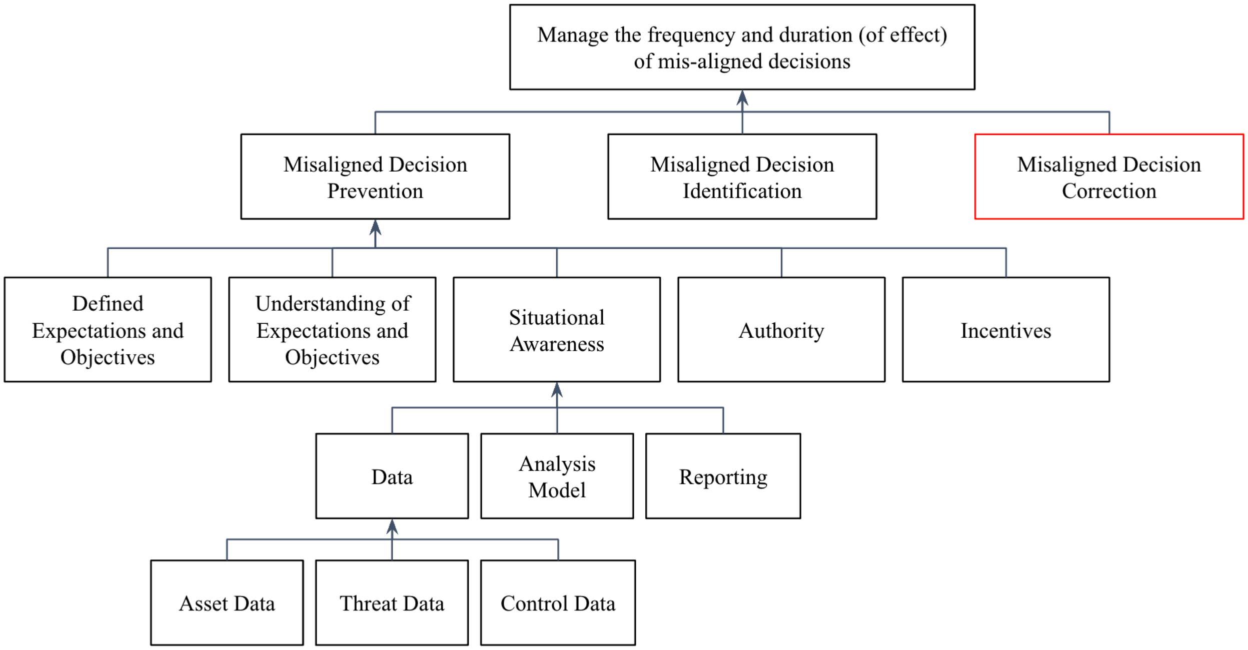
Example Controls

- Policy reviews
- Policy exception approval reviews
- Risk management program reviews
- Audits
- Incident postmortems
- Root cause analysis

Unit of Measurement

The amount of elapsed time from when a misaligned decision was made and its identification.

5.3 | Correcting Misaligned Decisions


Manage the frequency and duration (of effect) of mis-aligned decisions
Misaligned Decision Prevention
Misaligned Decision Identification
Misaligned Decision Correction
Defined Expectations and Objectives
Understanding of Expectations and Objectives
Situational Awareness
Authority
Incentives
Data
Analysis Model
Reporting
Asset Data
Threat Data
Control Data

Function Description

"Correct the causes and outcomes of misaligned decisions."

Discussion

Misaligned decisions have causes and outcomes. Correcting the outcomes tends to be simpler and more straightforward than correcting the causes, which often requires some form of root cause analysis. For example:

- If a decision is made to choose a password that doesn't meet the expectations of the organization, the outcome is a variant condition. Correcting that variance is accomplished in Variance Correction. The cause of that variance may be deficient training, insufficient incentives, etc., which are themselves variant conditions that also would be corrected through Variance Correction.

- If a decision is made to click on an illicit email attachment, correcting the outcome of that decision may involve Loss Event Response controls. Correcting the deficiencies that resulted in that decision to click on the attachment may require root cause analysis and the correction of one or more contributing deficiencies (e.g., updating policies, improving training, improving threat intelligence, etc.) which tend to involve Variance Management or Decision Support Prevention controls.

Consequently, there are no distinct controls that serve this function.

Relationships and Dependencies

Because this function is fulfilled by controls within other functions, it is wholly dependent upon those other functions.

Example Controls

N/A

Unit of Measurement

The amount of elapsed time between when a misaligned decision was recognized and corrected.