HITRUST Approach to Quasi-Quantitative Residual Risk Analysis (QQRRA)

Quantifying Risk in a Qualitative World

July 2022

Patent Pending Methodology

Unique HITRUST Quasi-Quantitative Residual Risk Analysis (QQRRA) model and computational approach provides a realistic cost-based analysis of information security, privacy, and compliance risk using an organization's current and target cybersecurity profiles.

Executive Summary

Since its inception in 2007, the HITRUST Approach[1] has become one of the most successful private-sector solutions for organizational and third-party risk management, in large measure due to HITRUST's ongoing dedication to meet the evolving needs of all industries through continuous improvement. These program enhancements are typically focused on providing our stakeholder community with complementary tools and methodologies to support diverse types of risk analyses. By tying HITRUST CSF®[2] controls to specific threats and assets and expressing risk in the language of business, i.e., financial impact, organizations can improve the accuracy and precision of the risk analyses needed for ongoing risk-based management of their HITRUST CSF control environment, including those conducted to evaluate control gaps, select alternate controls, prioritize corrective actions, or accept additional risk.

This paper addresses relevant concepts around information risk and its relationship to organizational risk and enterprise risk management, control framework-based risk analysis and control specification, threat to control relationships, and general risk concepts such as risk capacity, appetite, tolerance, and targets. After addressing the decomposition of risk and the specific assumptions made during development, we present the HITRUST patent pending Quasi-Quantitative Residual Risk Analysis (QQRRA) model and computational approach followed by an example analysis of a single threat, ransomware.

Through the provision of a standardized approach to quantitative, control-based risk management, HITRUST can help organizations make better informed management decisions, ensure scarce resources are expended more efficiently and effectively, improve regulatory compliance and the protection of sensitive information, better communicate risk to its many stakeholders, and ultimately reduce the overall cost of their information risk management programs.

[1] HITRUST (2022a). The HITRUST Approach.
[2] HITRUST (2022b). HITRUST CSF.

Acknowledgements

The author would like to thank Mr. Omar Khawaja, the Chief Information Security Officer at Highmark Health,[3] for encouraging HITRUST to develop a quantifiable approach to risk analysis that fully leverages the HITRUST Approach and, in particular, HITRUST Assessments. And, of course, special thanks go out to HITRUST Chief Executive Officer, Daniel Nutkis, for supporting the work on what has become something of a 'passion project' for me.

[3] Highmark (2022). Your Health Care Partner.

Table of Contents

Introduction 8

Background 8

Current Limitations 9

A New Approach 10

Relevant Concepts 11

Risk 11

Information Risk 12

Control Framework-based Risk Analysis 13

Threat-to-Control Mappings 14

Control Functions 14

NIST Cybersecurity Framework 15

Control Maturity and Scoring Model 18

Calculating Risk 19

Quasi-Quantitative Residual Risk Analysis (QQRRA) 20

Risk Model 20

Risk Decomposition 20

Control Function Decomposition 20

Risk Ontology 22

Computation Model 23

Operational (Direct) Risk 23

Non-Operational (Indirect) Risk 28

The Calculus 29

Assumptions 29

General Approach 29

Risk Tables 30

Worked Example 37

Contextual Analysis - Baseline 37

Calculating Operational (Direct) Risk 38

Calculating Non-Operational (Indirect) Risk 40

Calculating Total Risk 41

Contextual Analysis - Current Profile 41

Table of Contents

Calculating Operational (Direct) Risk 42

Calculating Non-Operational (Indirect) Risk 42

Calculating Total Risk 43

Calculating Risk Reduction 43

Flexibility of Approach 43

Limitations 43

About the Author 45

About HITRUST 45

Appendix A - Acronyms 46

Appendix B - Glossary 50

Appendix C - References 62

Table of Contents

List of Figures

Figure 1. Qualitative Risk Matrix 8

Figure 2. Quasi-quantitative Risk Matrix 8

Figure 3. Risk Concepts 11

Figure 4. The Relationship of Information and Organizational Risk 12

Figure 5. Control Framework-based Risk Analysis 13

Figure 6. HITRUST Threat Ontology 14

Figure 7. NIST Cybersecurity Framework Core 16

Figure 8. Using the HITRUST CSF to Support NIST Cybersecurity Framework Implementation 17

Figure 9. HITRUST Control Maturity Model 18

Figure 10. Basic Risk Decomposition Model 20

Figure 11. QQRRA Risk Decomposition Model 20

Figure 12. Relationship Between the NIST Core Functions and Control Functions 20

Figure 13. Relationship of the NIST Core Identify Function with Other NIST Core Functions 21

Figure 14. QQRRA Control Function Decomposition Model 22

Figure 15. QQRRA Risk Ontology 23

Figure 16. Annualized Loss Expectancy Model 24

Figure 17. Attentuating Annual Rate of Occurrence in the ALE Model 24

Figure 18. Threat Actor Motivation and Capability in the ALE Model 25

Figure 19. Modifying Motivation and Capability to Attentuate ARO in the ALE Model 25

Figure 20. Incorporating Probability into the ALE Model 26

Figure 21. QQRRA Operational (Direct) Risk Computation Model 27

Figure 22. QQRRA Non-operational (Indirect) Risk Computation Model. 28

Figure 23. Applying Decision Support and Variance Reduction Controls to the Implementation Maturity Model 29

Figure 24. The HITRUST Approach 45

Table of Contents

List of Tables

Table 1. Measurement Scale 30

Table 2. Relationship Between Frequency and Probability 31

Table 3. Real World Examples of Frequency and Probability Categories 31

Table 4. Real World Examples of Frequency and Probability Categories (Rare) 32

Table 5. Motivation Scale 33

Table 6. Capability 34

Table 7. Skills 34

Table 8. Resources 35

Table 9. Secondary Event Probability 35

Table 10. Impact Categories and Quantitative Scales 36

Table 11. Contextual Example of Impact Categories and Scales 37

Table 12. Example HITRUST Assessment Results (Baseline Analysis) 38

Table 13. Example of HITRUST Assessment Results (Contextual Analysis) 41

Table 14. Risk Reduction (Compared to Baseline) 43

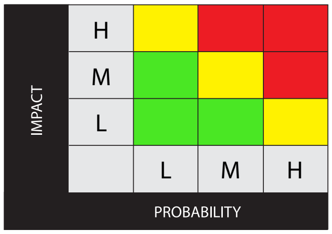
Introduction

Many organizations rely on qualitative approaches to evaluating and communicating risk that simply do not answer some of the most important questions organizations should ask. For example, "Are we protecting information better than last year?" "How much risk did we reduce through our investments in information security?" This paper proposes a quasi-quantitative approach that addresses the shortcomings of traditional qualitative approaches to help organizations provide better answers and manage information security risks in a more efficient and cost-effective way.

Background

There are three general approaches to risk analysis: qualitative, semi- or quasi-quantitative, and quantitative.

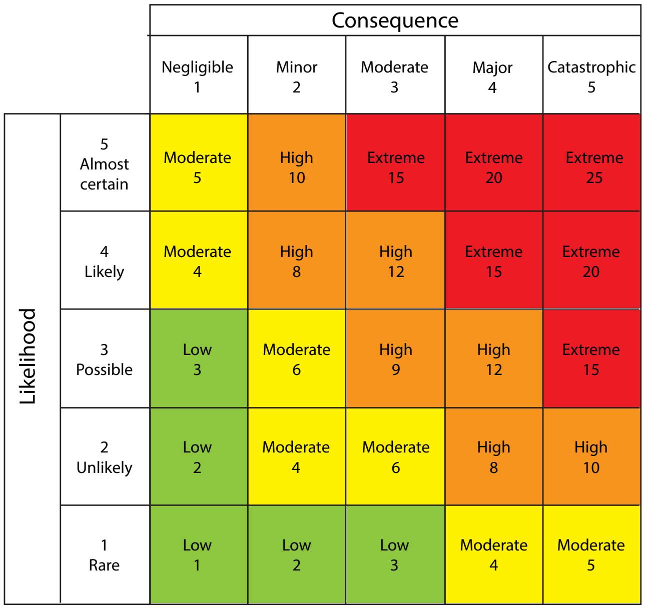
Qualitative approaches generally categorize elements of a risk analysis model (e.g., as low, medium, or high), and relationships between these elements are typically addressed by using various types of tables or matrices such as the one shown here.



IMPACT				
	H	🟨	🟥	🟥
	M	🟩	🟨	🟥
	L	🟩	🟩	🟨
		L	M	H
		PROBABILITY		

Figure 1. Qualitative Risk Matrix

Semi- or quasi-quantitative approaches generally assign values to the categories for each element in the risk analysis, and simple computations—either additive or multiplicative—are made based on those numbers, as shown below.



		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 15	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Figure 2. Quasi-quantitative Risk Matrix

Quantitative methods, however, typically do not use categories and values for each element in the risk model and are estimated or computed directly. For example, actuarial tables and other sources of data might provide values for the likelihood of a specific incident occurring (e.g., theft of a laptop) and the estimated value of the resulting loss (e.g., cost of a stolen laptop as well as an estimate for breach-related losses for a specific number and type of sensitive records).

With respect to questions of risk reduction that result from the implementation and maintenance of controls; however, few approaches are available despite the existence of various schema that describe how controls address threats and subsequently help manage risk (e.g., controls may be preventive, detective, or corrective[4]). The converse is also true, as control-based risk management frameworks generally do not address how their controls actually mitigate risk (or by how much). This is generally left to the user of the framework to determine.

> *Whether you call them risk assessment frameworks or risk management frameworks, what they purport to do is provide a means for organizations to manage risk better. … To a large degree, these frameworks do provide value in the sense that they provide structure and guidance that help organizations implicitly manage risk better. … Where these frameworks are less useful are [sic] in helping the practitioner determine the significance of deficiencies. … Most of these frameworks spend very little time on the question of risk measurement.*[5]

HITRUST takes an approach to general risk analysis and control specification that relies on the risk analysis performed by the National Institute of Standards and Technology (NIST)[6] to develop its control baselines[7] for information with diverse types of sensitivity and criticality. By tailoring one of these NIST baselines through the integration and harmonization of multiple security and privacy standards, best practice frameworks and regulatory requirements, the HITRUST CSF serves as an industry-level tailored overlay that—by integrating relevant inherent risk factors—provides a reasonable and appropriate specification of security controls that helps inform an organization's risk target.

HITRUST also provides a catalogue of threats that are then mapped to HITRUST CSF controls based on their specification and underlying requirements, which illustrates how the controls are addressing risk.[8]

The HITRUST Assurance Program™ then provides a rigorous approach to assessing HITRUST CSF controls that helps organizations demonstrate an appropriate level of due care via an effective and efficient approach to providing assurances to internal and external stakeholders that is both repeatable and reproducible.

Current Limitations

Quasi-quantitative approaches can help, but often do not relay risk in terms the business understands. "What is the real difference between a risk scored at '3.2' versus a '3.5'?" "If we invest $1M in security to reduce my risk from a '3.5' to a '3.2', do we get a reasonable risk reduction for our investment?"

Quantitative approaches can certainly help address these questions; however, they typically require a significant amount of expertise and information, one or both of which are often in short supply for many organizations. As a result, they are often limited to addressing risk questions of limited scope and seldom useful for questions around how well the organization is managing risk more broadly.

While HITRUST has begun work on tying threats to HITRUST CSF controls,[9] HITRUST guidance on risk analysis[10] does not currently support a quantitative approach to the various analyses an organization should conduct to manage its information risk efficiently and effectively (e.g.,

[4] Richards, D., Oliphant, A., and Le Grand, C. (2005, Mar). Global Technology Audit Guide: Information Technology Controls (GTAG 1). Altamonte Springs, FL: The Institute of Internal Auditors, p. 3.

[5] Freund, J. and Jones, J. (2015). Measuring and Managing Information Risk: A FAIR Approach. New York: Elsevier, pp. 356-357.

[6] NIST (2022A). About NIST.

[7] Joint Task Force, JTF (2020, Oct). Control Baselines for Information Systems and Organizations (NIST SP 800-53B). Gaithersburg, MD: NIST.

[8] HITRUST (2021). HITRUST Threat Catalogue. Frisco, TX: Author.

[9] HITRUST (2022d).

[10] Cline, B. (2018, Feb).

corrective action planning/prioritization, risk acceptance, and analyses of alternate controls). Instead, HITRUST currently provides a mixed quasi-quantitative approach based on control maturity and impact ratings[11] to estimate the additional risk incurred when control requirements are not fully implemented (mature). Although useful, the approach does not provide the same level of accuracy and precision as a more quantitative analysis nor present the resulting risk or expected loss estimates in monetary terms, which is arguably the 'preferred language' of corporate boards.

And, while the FAIR Institute provides a detailed quantitative approach to risk analysis that addresses expected loss monetarily, the approach often requires a significant amount of customization that is only suitable to very targeted types of risk analyses.[12] Unlike the HITRUST Approach™, the FAIR approach does not lend itself to broader analyses of risk based on the state of an organization's implemented controls. However, it does address how controls interact with threats to mitigate risk at a conceptual level.

Prior to QQRRA, HITRUST's approach to risk analysis was limited to a very broad representation of the likelihood component of risk based on control implementation maturity and impact represented by relative rankings of their potential impact. HITRUST also does not currently map enumerated threats to specific requirements in each HITRUST CSF control nor specify how these requirements interact with specific threats.

The MITRE Corporation provides two threat-based models that could support risk analysis: ATT&CK and D3FEND. The ATT&CK framework provides a knowledge base of threat actor tactics and techniques that can be used as a foundation for threat models while the D3FEND framework enumerates various controls and how they might address specific threats. However, the MITRE frameworks are extremely granular and subsequently limited to supporting specific, targeted types of risk analyses around logical cyber-based threats.

A New Approach

In this paper, HITRUST presents its novel, patent pending approach to quasi-quantitative residual risk analysis, or QQRRA, that will help address many of the limitations in our current approach. More specifically, the QQRRA approach will:

- Support more granular quasi-quantitative risk analyses than the previous approach
- Support both simple types of analyses (single threat with multiple controls or single control with multiple threats) as well as more complex analyses (multiple threats and multiple controls)
- Integrate all controls and all levels of control implementation maturity across the risk model
- Provide value even when limited threat-related information is available
- Provide input into more rigorous quantitative risk analyses if needed

We accomplish this by leveraging (1) HITRUST's approach to control framework-based risk analysis in the specification and tailoring of HITRUST CSF controls that inform an organization's risk target, (2) the HITRUST Assurance Program as the basis for controls gap assessment and reporting of an organization's current state of protection, and (3) risk concepts that are well understood by industry to decompose risk and support a more granular quasi-quantitative risk computation model to help quantify risk reduction in monetary terms. This new integrated approach is easier to use than current approaches to quantitative analyses while providing more realistic estimates of risk than existing qualitative or quasi-quantitative approaches.

[11] Based on impact codes previously used by the U.S. Department of Defense (DoD). See Department of the Navy (2008, Jul 15). DoD Information Assurance Certification and Accreditation Process (DIACAP) Handbook, Version 1.0. Washington, D.C.: Author.

[12] Freund, J. and Jones, J. (2015).

Relevant Concepts

Risk

NIST defines risk as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and [is] typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence,"[13] which is consistent with our depictions of a qualitative and semi-quantitative risk matrix in the previous section. Basically, 'bad things can and do happen.' However, while information risk—at least from a security perspective—is often viewed negatively, one should always remember that risk may be both positive and negative. Gambling is a perfect example of this.

NIST also defines risk management as "the total process of identifying, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review."[14] Risk management is essentially all the things we do to manage our risk to a 'level' we find comfortable. For example, we may limit ourselves to $100 per night while gambling in Vegas and vow not to gamble any of our winnings (if we are lucky) from any prior night of gambling. Or we may be willing to 'lose it all.'

NIST then goes on to define risk analysis as "the process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact" and considers the term synonymous with risk assessment.[15] Risk analysis is what we do to determine the risks we need to control. For example, we may look at the expected payoffs and our relative skills for various forms of gambling, such as roulette and craps, in which we would like to engage. We may also recognize that drinking while gambling results in degraded judgment. And of course, it might be a good idea to consider how gambling could adversely impact the family budget.

This brings us to some important but sometimes misunderstood concepts around risk tolerance, appetite, and capacity.

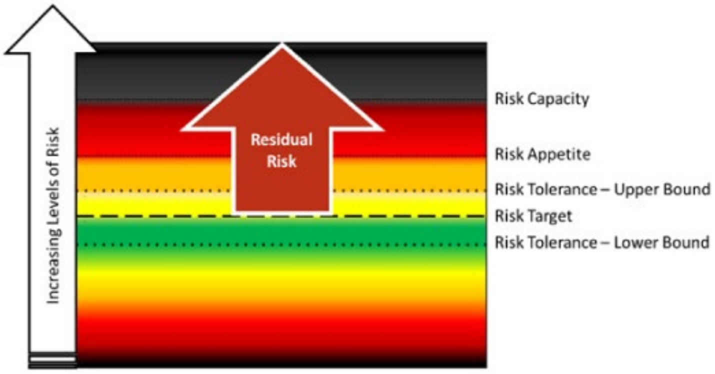

Increasing Levels of Risk
Residual Risk
Risk Capacity
Risk Appetite
Risk Tolerance – Upper Bound
Risk Target
Risk Tolerance – Lower Bound

Figure 3. Risk Concepts

Although depicted in the figure above, risk appetite is actually a qualitative description of an organization's willingness to accept a certain amount of risk to achieve its objectives. However, it is used to set risk tolerances, which is a quantitative measure of the levels of risk taking it would consider acceptable in the pursuit of a specific objective or to manage a certain category of risk. As one might expect, tolerable risk exists between the lower and upper bounds of an organization's risk tolerance around its risk target. (Recall that not all risk is negative. One may wish to control less risk if the dollars would be better spent elsewhere.)

Residual risk is risk that is not controlled. If all controls specified by an organization's risk analysis are implemented, residual risk should only exist above the organization's risk target(s). If it is also below the upper bound of risk tolerance, the residual risk would, by definition, be tolerable (i.e.,

[13] NIST (2022b). Information Technology Laboratory: Computer Security Resource Center: Glossary.

[14] Ibid.

[15] Ibid.

acceptable) to the organization. Residual risk becomes intolerable (unacceptable) if it exceeds the upper bound. And finally, the organization's risk appetite and tolerances should always be below its risk capacity, i.e., the maximum amount of risk it can absorb without disrupting the achievement of its business strategies and objectives.

Information Risk

Enterprise risk is a relatively broad term that addresses five major types of risk: strategic, reputational, operational, compliance, and financial.[16] While some of these risks have no clear 'bright line,' such as the view that reputational risk can be viewed as a strategic risk, this categorization allows risk managers to think of risk across the enterprise more holistically than they otherwise might.

Information risk is also something that is less understood by executive management than these more 'traditional' forms of organizational risk; however, HITRUST views information risk through the lens of these other risks as shown in Figure 4 on the next page.

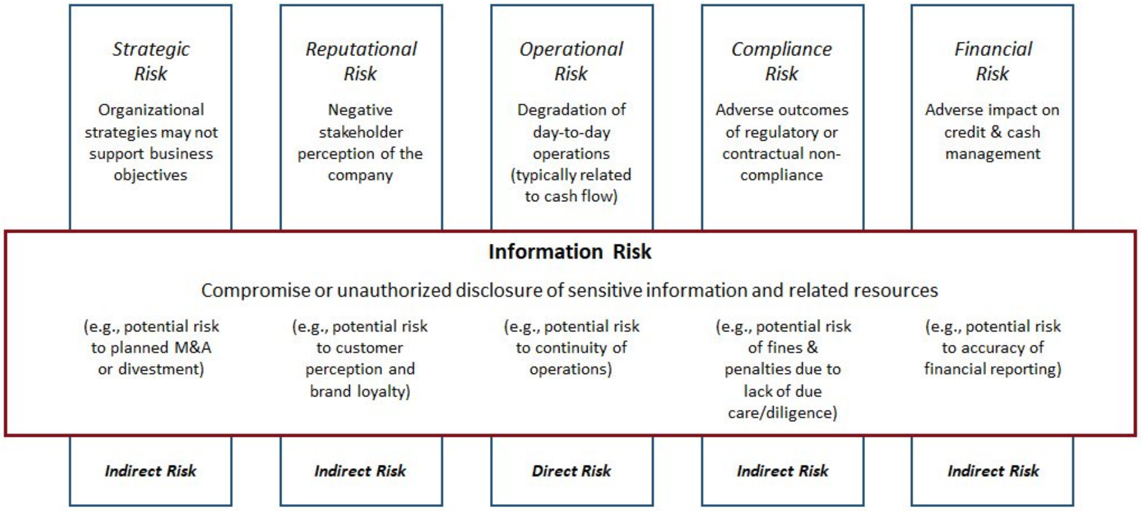

Strategic Risk
Organizational strategies may not support business objectives
Reputational Risk
Negative stakeholder perception of the company
Operational Risk
Degradation of day-to-day operations (typically related to cash flow)
Compliance Risk
Adverse outcomes of regulatory or contractual non-compliance
Financial Risk
Adverse impact on credit & cash management
Information Risk
Compromise or unauthorized disclosure of sensitive information and related resources
(e.g., potential risk to planned M&A or divestment)
(e.g., potential risk to customer perception and brand loyalty)
(e.g., potential risk to continuity of operations)
(e.g., potential risk of fines & penalties due to lack of due care/diligence)
(e.g., potential risk to accuracy of financial reporting)
Indirect Risk
Indirect Risk
Direct Risk
Indirect Risk
Indirect Risk

Figure 4. The Relationship of Information and Organizational Risk

We can further classify these forms of information risk (and potential loss) as either directly or indirectly attributable to an incident.

Although some frameworks include legal and regulatory/compliance risks along with write downs, loss of recourse, restitution, and loss or damage of assets in their definition of direct operational risk,[17] the ERM model we use gives them their own category of risk. We also classify them as indirect since such losses result from a decision made by another stakeholder. And, of the two types of operational losses that could be classified as indirect—near miss and latent losses—the former means losses were successfully avoided and the latter means losses are unrealized, i.e., asset values could potentially recover, and we discount them as well. We subsequently classify operational risk, in general, as direct risk and other forms of enterprise risk as indirect risk.

[16] Stine, K., Quinn, S., Witte, G., and Gardner, R. (2020, Oct). Integrating Cybersecurity and Enterprise Risk Management (ERM) (NISTIR 8286). Gaithersburg, MD: NIST, pp. 4, 42-43.

[17] Banking and Financial Services BA (2012, May 10). Basil II – Direct vs. Indirect Operational Loss (Blog).

Control Framework-based Risk Analysis

The primary output of a broad-based risk analysis is the specification of controls to address threats to sensitive and/or critical information.[18] NIST provides a series of three baselines that are selected based on the information's sensitivity and criticality, which is commensurate with the potential adverse impact to an organization due to a loss of information confidentiality, integrity, and/or availability. Regardless, any baseline selected will require further tailoring (customization).[19,20] By going through the tailoring process NIST outlines, organizations can create overlays of a control baseline to suit their specific needs.

HITRUST followed a tailoring process similar to that used to create other overlays, such as the one used by the Centers for Medicare and Medicaid Services [CMS] to create their Acceptable Risk Safeguards,[21] to create a new, enhanced overlay for general use by industry—the HITRUST CSF. Organizations can tailor the HITRUST CSF even further based on relevant inherent risk factors, which include but are not limited to the type and amount of information processed, how that information is processed, and by whom.[22,23]

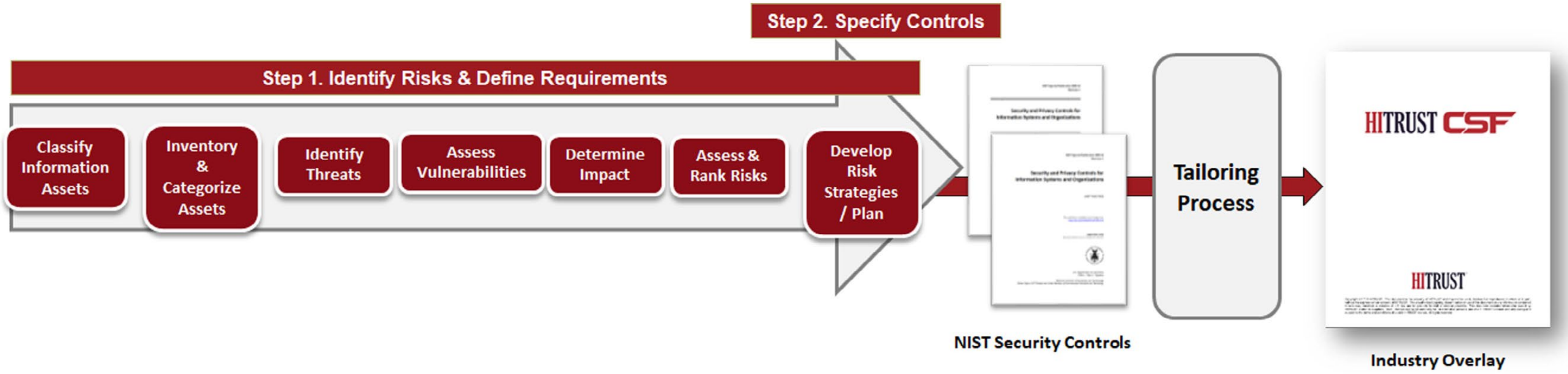


Figure 5. Control Framework-based Risk Analysis

The benefit of leveraging a recognized control framework such as the one provided by NIST is that it allows organizations to generate a reasonable and appropriate set of controls that help provide an acceptable level of protection for sensitive and/or critical information much easier than if they were to conduct their own comprehensive risk analysis 'from scratch.' Further, when inherent risk factors are applied to tailor HITRUST CSF control requirements based on its inherent risks, the resulting control specification helps establish an organization's target profile and subsequently its risk target.[24]

[18] Joint Task Force Transformation Initiative, JTF TI (2011, Mar). Managing Information Security Risk: Organization, Mission, and Information System View (NIST SP 800-39), §3.3

[19] NIST (2004). Standards for Security Categorization of Federal Information and Information Systems (FIPS Pub 199). Gaithersburg, MD: Author.

[20] Joint Task Force, JTF (2020, Oct). Control Baselines for Information Systems and Organizations (NIST SP 800-53B). Gaithersburg, MD: NIST.

[21] Centers for Medicare and Medicaid Services, CMS (2017). CMS Acceptable Risk Safeguards (ARS) (CMS_CIO-STD-SEC01-3.0). Baltimore, MD: Author.

[22] Cline, B. (2017, Sep). Leveraging a Control-Based Framework to Simplify the Risk Analysis Process, ISSA Journal, 15(9), pp. 39-42.

[23] Cline, B. (2018, Feb). Risk Analysis Guide for HITRUST Organizations & Assessors: A guide for self and third-party assessors on the application of HITRUST's approach to risk analysis. Frisco, TX: HITRUST.

[24] The comprehensive and scalable HITRUST CSF framework is available for eligible organizations to download free of charge from the HITRUST website.

Threat-to-Control Mappings

Controls are implemented specifically to address one or more threats and subsequently the risk associated with those threats. To help organizations understand the threats their HITRUST CSF control specification is addressing, HITRUST provides a four-level threat taxonomy consisting of threats, threat subcategories, threat categories, and threat types. The classification schema—shown in the figure below—supports a mutually exclusive and collectively exhaustive enumeration of threats to sensitive information articulated at a level commensurate with the granularity of the HITRUST CSF control requirements to which they are mapped.

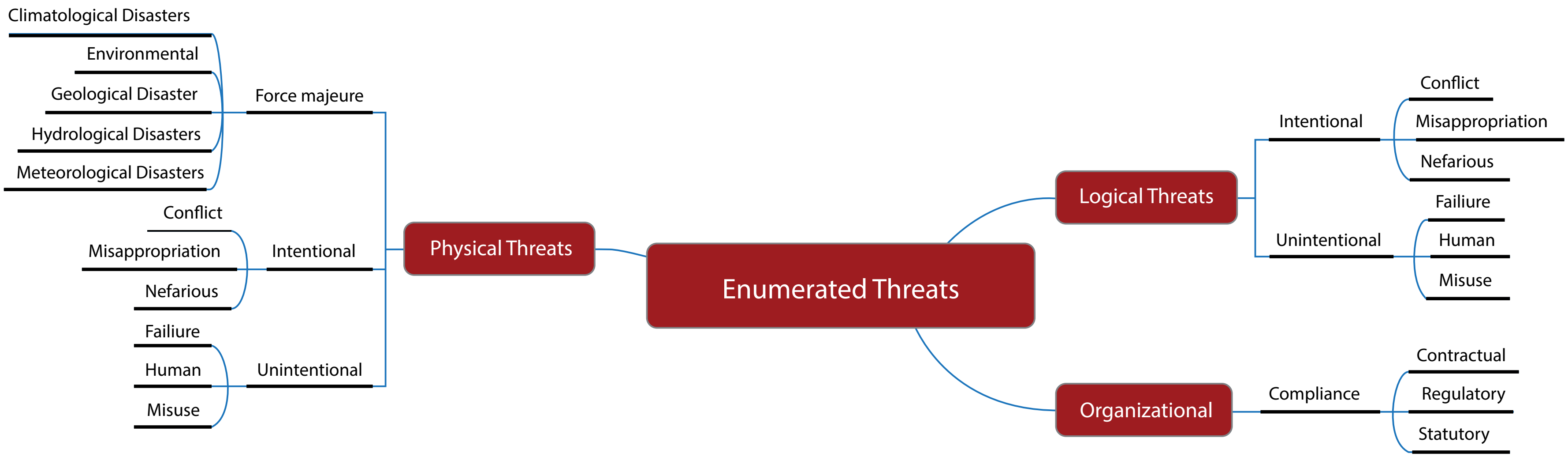


Figure 6. HITRUST Threat Ontology[25]

Control Functions

As pointed out earlier, controls interact with threats in different ways and the ways in which they interact help determine a control's function. The most basic categorization of control functions consists of preventive, detective, and corrective controls,[26] where:

- Preventive controls act to stop a threat event from occurring,
- Detective controls act to identify when a threat event occurs, and
- Corrective controls act to limit the potential impact of a threat event once it has occurred.

[25] HITRUST (2021).

[26] Richards, D., Oliphant, A., and Le Grand, C. (2005, Mar), p. 3-4.

Other approaches to categorizing control functions generally expand on these three.

For example, one approach splits corrective controls into two separate components:[27]

- Response Controls – Address errors or irregularities due to the detected threat event
- Recovery Controls – Restore systems back to pre-threat event conditions

Another approach adds the concept of addressing a threat by affecting the threat actor:[28]

- Deterrent Controls – Discourage a threat actor from initiating a threat event

The concept of deterrent controls is somewhat similar to another approach that focuses on an organization's workforce, whether as a positive force to enhance security or as a potential threat actor:[29]

- Directive Controls – Establish desired requirements or guidelines intended to produce specific outcomes based on policies and procedures.

Preventive controls are split into three separate components in yet another approach and, in addition to deterrent controls, include:[30]

- Avoidance Controls – Reduce the frequency with which a threat actor comes into contact with an asset
- Resistive Controls – Make a threat agent's job more difficult (in a malicious or act-of-nature scenario) or easier (in a human error scenario)

The same approach also defines two additional 'quality performance' oriented control functions:

- Decision-making Controls – Improve the quality of risk-related decision-making
- Variance Controls – Reduce variability in the performance (effectiveness) of other controls

NIST Cybersecurity Framework

The NIST *Framework for Improving Critical Infrastructure Cybersecurity*[31] (NIST Cybersecurity Framework) is an overarching risk management framework that leverages other frameworks, standards, guidelines, and best practices to address an organization's information (cybersecurity) risk.

Essentially, the NIST Cybersecurity Framework helps organizations:

- Ensure people, process, and technology elements completely and comprehensively address information and cybersecurity risks consistent with their business objectives, including legislative, regulatory, and best practice requirements;
- Identify risks from the use of information by the organization's business units and facilitate the avoidance, transfer, reduction, or acceptance of risk; and
- Support policy definition, enforcement, measurement, monitoring, and reporting for each component of the security program and ensure these components are adequately addressed.

[27] Williams, C., Donaldson, S., and Siegal, S. (2020). Building an Effective Security Program. Boston: De Gruter.

[28] Miller, L. and Gregory, P. (2012). CISSP for Dummies (4th ed.). New York: Wiley.

[29] Lartey, P., Kong, Y., Bah, F., Santosh, R., and Gumah, I. (2019, Aug). Determinants of Internal Control Compliance in Public Organizations; Using Preventive, Detective, Corrective and Directive Controls. In International Journal of Public Administration, p. 4.

[30] Freund, J. and Jones, J. (2015).

[31] NIST (2018, 16 Apr). Framework for Improving Critical Infrastructure Cybersecurity (v1.1). Gaithersburg, MD: Author.

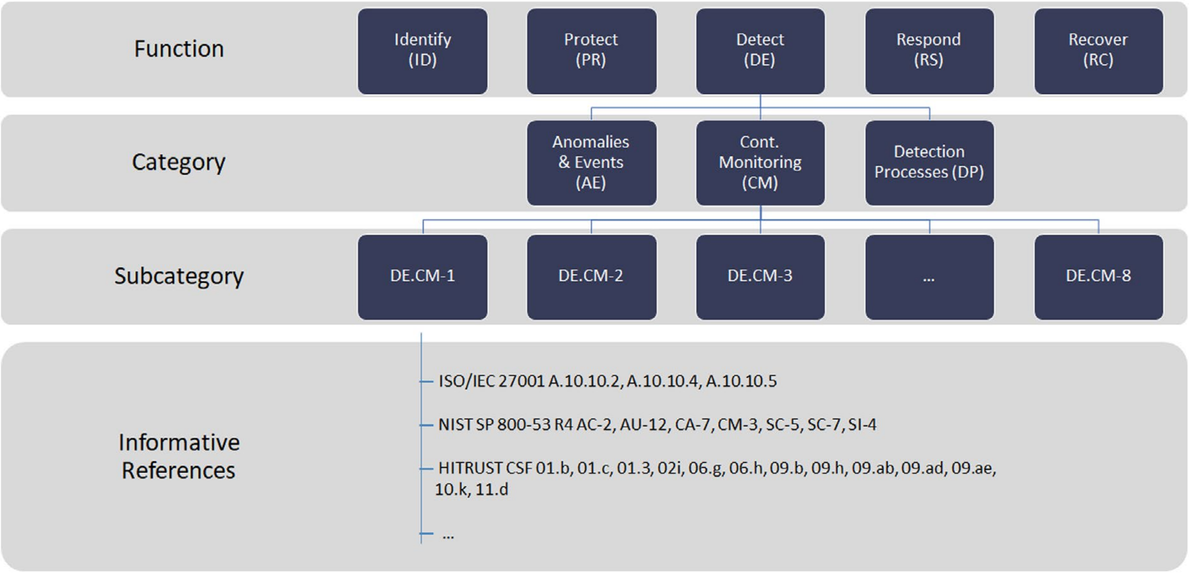


Figure 7. NIST Cybersecurity Framework Core

A principal component of the NIST Cybersecurity Framework is the Framework Core, depicted in the figure above, which provides the overarching structure for the assignment of cybersecurity activities that support specific cybersecurity outcomes.

The Framework Core is comprised of four elements:[32]

- **Functions** organize basic cybersecurity activities at their highest level and help organizations manage cybersecurity risk.
  - *Identify* – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
    - "The activities in the Identify Function are foundational for effective use of the Framework.
    - "Examples of outcome Categories within this Function include Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
  - *Protect* – Develop and implement appropriate safeguards to ensure delivery of critical services.
    - "The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.
    - "Examples of outcome Categories within this Function include Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
  - *Detect* – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
    - The Detect Function enables timely discovery of cybersecurity events.
    - Examples of outcome Categories within this Function include Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
  - *Respond* – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
    - The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.
    - Examples of outcome Categories within this Function include Response Planning; Communications; Analysis; Mitigation; and Improvements.
  - *Recover* – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
    - The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.
    - Examples of outcome Categories within this Function include Recovery Planning; Improvements; and Communications.

[32] Ibid.

- **Categories** subdivide Functions into groups of cybersecurity outcomes that are topical in nature.
- **Subcategories** further subdivide Categories into specific cybersecurity outcomes.
- **Informative References** are standards, frameworks, guidelines, and best practices that support the outcomes specified by each subcategory.[33,34]

The figure below depicts how specific types of Informative References relate to the NIST Cybersecurity Framework Core and can subsequently be used to help specify the controls needed to help organizations achieve the cybersecurity outcomes articulated by the NIST Subcategories.

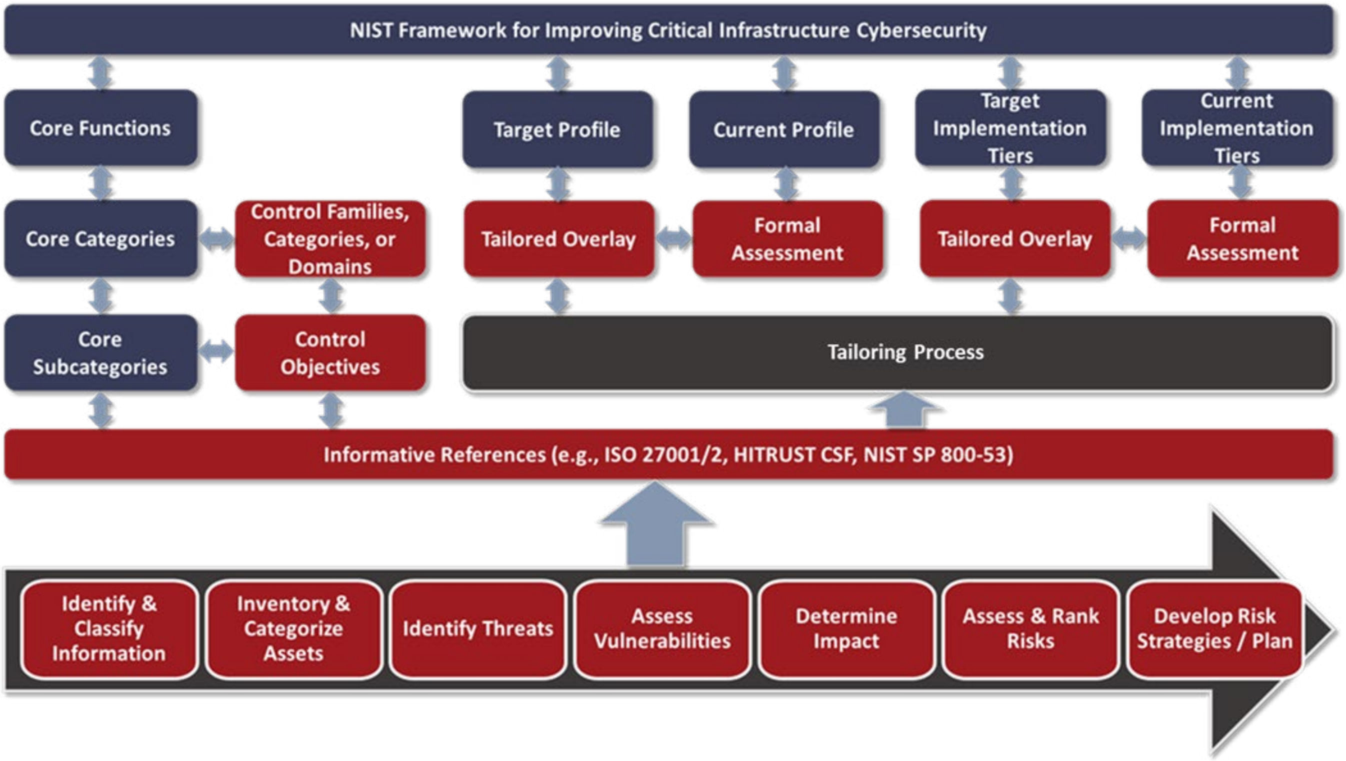

NIST Framework for Improving Critical Infrastructure Cybersecurity
Core Functions
Target Profile
Current Profile
Target Implementation Tiers
Current Implementation Tiers
Core Categories
Control Families, Categories, or Domains
Tailored Overlay
Formal Assessment
Tailored Overlay
Formal Assessment
Core Subcategories
Control Objectives
Tailoring Process
Informative References (e.g., ISO 27001/2, HITRUST CSF, NIST SP 800-53)
Identify & Classify Information
Inventory & Categorize Assets
Identify Threats
Assess Vulnerabilities
Determine Impact
Assess & Rank Risks
Develop Risk Strategies / Plan

Figure 8. Using the HITRUST CSF to Support NIST Cybersecurity Framework Implementation

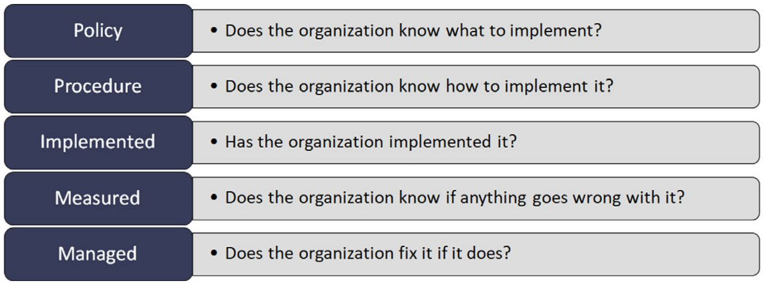
The HITRUST CSF is a recognized NIST Cybersecurity Framework Core Informative Reference[35] and serves as the foundation for the first Healthcare and Public Health (HPH) sector[36] guide on implementation of the NIST Cybersecurity Framework,[37] which was first developed and published in 2016 by the Critical Infrastructure Protection Advisory Council (CIPAC[38]) HPH Sector Coordinating Council (SCC[39]) Joint HPH Cybersecurity Working Group (WG) Risk Management Sub-WG.

[33] Ibid., pp. 6 – 8.
[34] Emphasis and bulleted structure added.
[35] NIST (2022c). National Online Informative References Program: Informative Reference Catalog.
[36] Public Health Emergency, PHE (2022). Preparedness: Planning: Critical Infrastructure Protection: [HPH] Sector.
[37] Joint HPH Cybersecurity WG (2016, May). Healthcare Sector Cybersecurity Framework Implementation Guide.
[38] Cybersecurity & Infrastructure Agency, CISA (2022a). Critical Infrastructure Partnership Advisory Council.
[39] CISA (2022b). Infrastructure Security: Critical Infrastructure Sector Partnerships: Sector Coordinating Councils.

Control Maturity and Scoring Model

There are many ways to evaluate a control's implementation, the simplest of which is to determine if the control is fully implemented or not.

HITRUST uses a five-level control maturity implementation model[40] based on NIST guidance,[41] as shown below.



Policy	• Does the organization know what to implement?
Procedure	• Does the organization know how to implement it?
Implemented	• Has the organization implemented it?
Measured	• Does the organization know if anything goes wrong with it?
Managed	• Does the organization fix it if it does?

Figure 9. HITRUST Control Maturity Model

Scoring for the maturity levels can be equal or weighted, e.g.:

- Policy – 15 pts
- Procedure – 20 pts
- Implemented – 40 pts
- Measured – 10 pts
- Managed – 15 pts

The number of points awarded for each maturity level is based on the level of compliance evaluated:

- Non-Compliant (NC) – 0% of points awarded
- Somewhat Compliant (SC) – 25% of pts awarded
- Partially Compliant (PC) – 50% of pts awarded
- Mostly Compliant (MC) – 75% of pts awarded
- Fully Compliant (FC) – 100% of pts awarded

Compliance may also be based on two (compliant, non-compliant), three (compliant, partially compliant, non-compliant), or some other reasonable number of levels to provide an appropriate level of 'rely-ability,' i.e., the ability to rely upon the assurances provided by the approach.

The level of compliance is also based on specific implementation criteria related to each level of maturity.

[40] Cline, B., Huval, J., and Sheth, B. (2019, Oct). Evaluating Control Maturity Using the HITRUST Approach: Quasi-quantitative scoring based on the HITRUST CSF security and privacy control implementation maturity model.

[41] Bowen, P. and Kissel, R. (2007, Jan). Program Review for Information Security Management Assistance (PRISMA) [NISTIR 7358]. Gaithersburg, MD: NIST, pp. 2-3.

Calculating Risk

Risk, R, is generally considered to be a function of the likelihood, L, a threat will successfully exploit a vulnerability and the probable impact, I, should it occur. Likelihood is generally expressed as a probability and impact is provided in various forms although monetary values are preferred. Risk is often expressed as a simple multiplicative function, whether the computation is performed quantitatively or qualitatively (via an 'n x n' matrix as shown previously in the introduction).

$$R = L \times I$$

An alternate approach forgoes the use of probability in favor of frequency or rate of occurrence, which can be estimated based on how often an event is observed in a specified time period. Called annualized loss expectancy, ALE, it is expressed as a function of the annual rate of occurrence, ARO, and the single loss expectancy, SLE, i.e., the expected loss to an asset from a single occurrence of the event.[42]

The model also recognizes an adverse event may not and probably would not result in the total loss of an asset. For example, a brick building may suffer less damage from a fire than one made entirely of wood, and one building may suffer less damage due to having fire control and response mechanisms as opposed to another building identical to the first in every other way. Subsequently asset value, AV, is modified by an exposure factor, EF, to reflect the probable loss as opposed to the possible loss.

$$ALE = ARO \times SLE = ARO \times (AV \times EF)$$

ALE is expressed as dollars per year, ARO is simply the number of times one might expect to see the event occur per year, AV is expressed in dollars, and EF is unitless as it is generally provided as a percentage.

[42] Hansche, S., Berti, J., and Hare, C. (2004). Official (ISC)2 Guide to the CISSP Exam. Boca Raton, FL: Auerbach.

Quasi-Quantitative Residual Risk Analysis (QQRRA)

Risk Model

Risk Decomposition

As was evident in our introduction and subsequent discussion of risk, there are two principal elements of risk: the likelihood a threat event will occur and the probable (adverse) impact if it does.

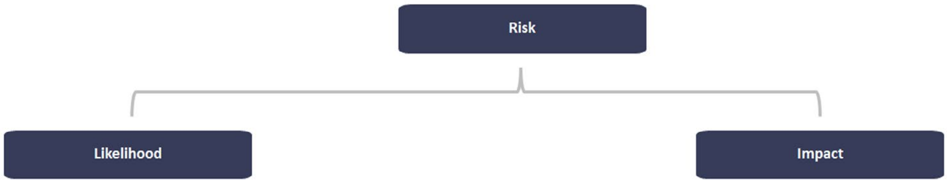


Figure 10. Basic Risk Decomposition Model

To further decompose likelihood and impact, one can model the risk that results from a specific threat using a 'threat statement. 'While these statements may vary in form, they are almost always similar in substance. HITRUST used such a threat statement when vetting high-level threats enumerated in the original HITRUST Threat Catalogue published in 2016 and we use a similar statement here.

A Threat Actor Initiates a Threat by Exploiting a Vulnerability that Results in a Risk to an Asset of a Potential Loss

This results in a second-tier decomposition of risk as shown in the following figure.

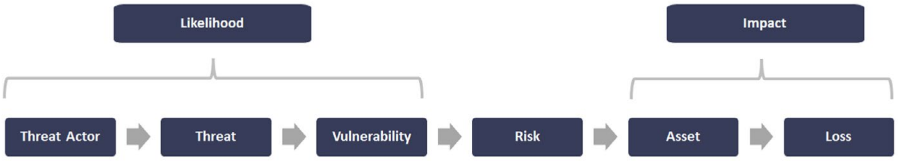


Figure 11. QQRRA Risk Decomposition Model

Control Function Decomposition

The NIST Cybersecurity Framework Core Functions have a prima facia similarity with many of the control functions we identified previously and can be mapped as shown in the figure below.

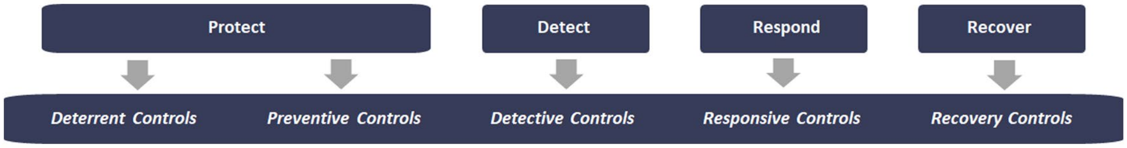


Figure 12. Relationship Between the NIST Core Functions and Control Functions

While the NIST Cybersecurity Core Identify Function's relationship to control functions is not as clear as the other functions, it is possible to ascertain their relationships based on the Core Categories that support the Core Functions.[43]

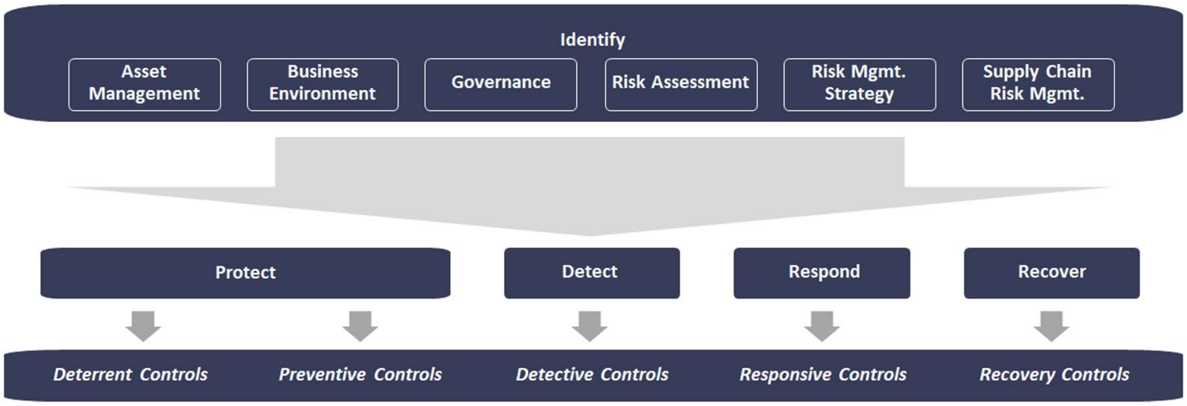


Figure 13. Relationship of the NIST Core Identify Function with Other NIST Core Functions[44]

Since "the activities in the Identify Function are **foundational** [emphasis added] for effective use of the Framework,"[45] we can assert that controls in the Identify Function generally support controls in the other Core Functions. For example:

1. *Asset management* ensures the organization knows what assets to protect, monitor, and subsequently reconstitute when a threat event is detected
2. An understanding of the *business environment* is needed to provide a meaningful context for organizational governance and management of all controls regardless of function
3. *Governance* helps ensure operational decisions regarding the management of controls, regardless of function, are made in alignment with the organization's mission and goals
4. *Risk assessment* is required to understand the risks that must be controlled to achieve business objectives and how to control them (vis-à-vis the specification of all necessary controls, regardless of function)
5. *Risk management (strategy)* is needed to actively control risk within the organization's general appetite and specific (quantifiable) tolerances for risk (using all specified controls, regardless of function)
6. *Supply chain risk management* (SCRM)[46] is needed to understand the risks posed by third parties and help ensure those risks are adequately controlled (using all relevant controls, regardless of function)

However, the question remains as to how these foundational activities interact with threats, i.e., what control functions do we assign them? Based on the managerial nature of most of the NIST Core Categories enumerated above, one might want to assign the directive control function presented earlier. However, there is more to these 'management type' controls than simply policy and procedure, the effect of which is generally limited to the organization's workforce (with limited exception, such as customers, business partners, and vendors based on a legal contract or other agreement). To see why, we can look to a few relevant definitions of management.

Management may be defined as "a set of activities directed at the efficient and effective utilization of resources in the pursuit of one or more goals"[47] or as "a problem-solving process of effectively achieving organizational objectives through the efficient use of scarce resources in a

[43] For example, see Blum, D. (2020). Rational Cybersecurity for Business: The Security Leader's Guide to Business Alignment. Apress: Silver Springs, MD., Figure 1. Available from https://learning.oreilly.com/library/view/rational-cybersecurity-for/9781484259528/htmel/Cover.xhtml.

[44] Based on concepts provided by Blum, D. (2020), Ch. 9, as depicted in Figure 9-1.

[45] NIST (2018, 16 Apr), p. 8.

[46] More generally, third party risk management (TPRM).

[47] Van Fleet, D. and Seperich, G. (2013). Agribusiness: Principles of Management (International ed.) New York: CENGAGE, p. 24.

changing environment."[48] Inspection of these definitions indicate there are two specific aspects of management that help an organization achieve its goals and objectives: the *problem-solving* activities that make up related business processes and the business *processes* themselves.

Problem-solving is essentially a decision-making process, the desired outcome of which is a good decision. Subsequently, any control in the Identity Function Categories that *support decision-making* would help ensure decision-makers make good decisions about information risk.

A business process is "a collection of activities with the purpose of taking one or more business inputs and creating a specific business output."[49] Further, a 'good' business process (any process actually) is one that is well-controlled—i.e., measured, managed, and continuously improved—to *reduce variation* in the process output.[50]

We subsequently use 'decision support' and 'variance reduction' as the final two control functions in the QQRRA model and assign NIST Cybersecurity Framework Core Identity Categories as follows:

- Decision Support Controls: asset management, risk management, and SCRM
- Variance Reduction Controls: risk assessment, business environment, and governance

We may now update the figure on the previous page as shown below.

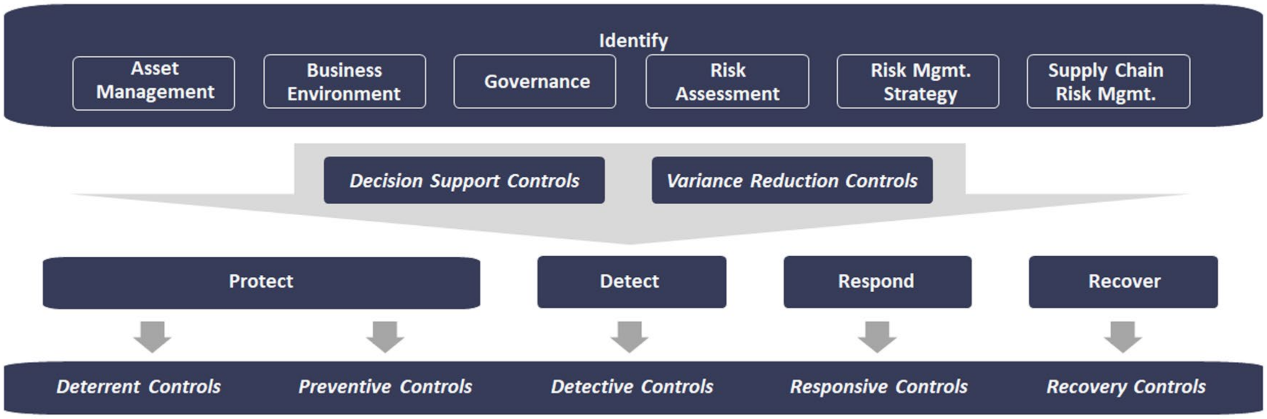


Figure 14. QQRRA Control Function Decomposition Model

Risk Ontology

We present the overall HITRUST QQRRA risk ontology by combining the QQRRA risk and control function decomposition models, the result of which is depicted in the figure on the next page.

[48] Kreitner, R. (1995). Management (6th ed.). New York: Houghton Mifflin College Division, p. 4.

[49] Law Insider (2022). Dictionary: Business Process.

[50] ASQ (2022A). Quality Resources: Six Sigma.

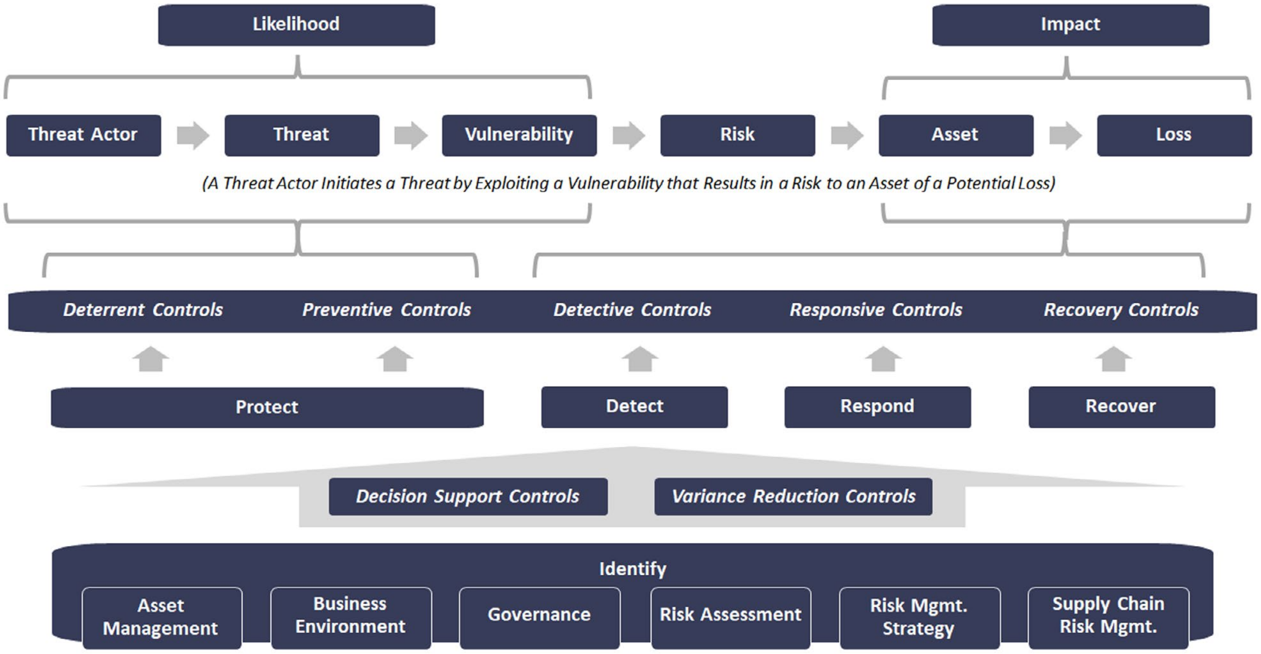


Figure 15. QQRRA Risk Ontology

Computation Model

Total risk consists of direct risk, i.e., that risk that is directly attributable to a threat event, and indirect risk, i.e., that risk that is incidental to and conditioned upon the direct risk. For information risk, we generally limit direct risk to operational risk, OR, and indirect risk to the other forms of enterprise risk, which we will now classify as non-operational risk, NR. We will subsequently compute OR as a function of the likelihood the initial threat event will occur and the probable impact and NR as a function of the conditional probability a second event will occur given the occurrence of the initial threat event and the probable impact of the secondary event. All types of loss relevant to a particular enterprise risk relevant to the event would be computed. And, although we present the model for a general use case, risk calculations are made for two or more control profiles to determine a change in residual risk. This will be addressed further in our discussion of the general approach to the analysis.

Although risk will be computed based on probabilities, we will start with the annualized loss expectancy, ALE, model and then build the OR computation model. The NR computation model will then be presented as a direct result of the OR model (modified for the conditional probability a second event will occur after the initial event).

Operational (Direct) Risk

The reason we start with the ALE approach is because organizations generally compute risk based on available information, whether observed internally or obtained externally from relevant surveys and other reports, on observed frequencies or rates of occurrence in addition to potential losses.

As stated previously, ALE is a function of annual rate of occurrence, ARO, and single loss expectancy, SLE, which in turn is derived from asset value, AV, and a relevant exposure factor, EF.

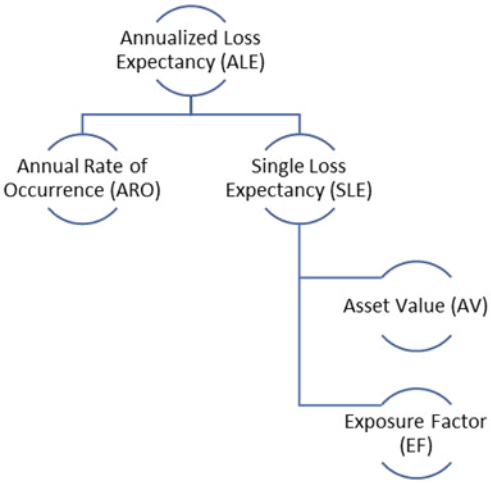

Annualized Loss Expectancy (ALE)
Annual Rate of Occurrence (ARO)
Single Loss Expectancy (SLE)
Asset Value (AV)
Exposure Factor (EF)

Figure 16. Annualized Loss Expectancy Model

However, we find the typical computation of ALE incomplete. Recall the threat statement, "A threat actor initiates a threat by exploiting a vulnerability. . . ." Since vulnerabilities exist regardless of the threat actor attempting to exploit them, we believe ARO is modified, i.e., the rate or frequency of occurrence is 'attenuated,' in the same way that AV is modified by an exposure factor to determine SLE as the probable loss in asset value.

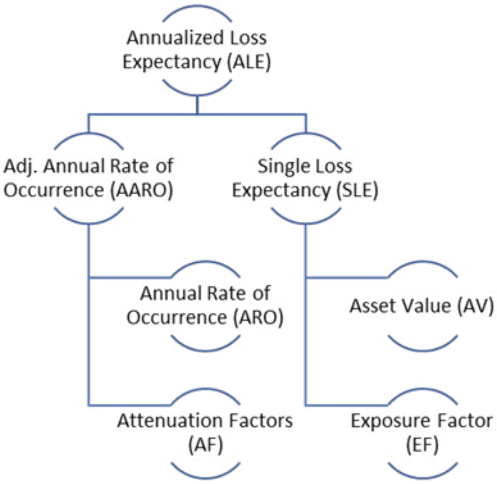

Annualized Loss Expectancy (ALE)
Adj. Annual Rate of Occurrence (AARO)
Single Loss Expectancy (SLE)
Annual Rate of Occurrence (ARO)
Attenuation Factors (AF)
Asset Value (AV)
Exposure Factor (EF)

Figure 17. Attenuating Annual Rate of Occurrence in the ALE Model

Further, a threat actor's ability to exploit a vulnerability, which impacts the likelihood and subsequently the frequency or rate of attack, may be attributed to two factors: the actor's motivation, M, and capability, C.[51]

- *A threat represents the motivation, capability, and opportunity of an adversary to attack or inflict harm*
- *Motivation is the desired reason (or reasons) an individual or group has for mounting an attack… [and] may involve political, cultural, financial, emotional, or other factors*
- *The attacker's capability refers to the knowledge, skills, and tools necessary to conduct an attack*
- *Opportunity represents the situational circumstances that would support the initiation of an attack*[52]

[51] Rossebo, J., Fransen, F., and Luiijf, E. (2016, Apr). Including threat actor capability and motivation in risk assessment for Smart Grids. IEEE Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG).

[52] CBRN Centres of Excellence (2015, Dec). How to Implement Security Controls for an Information Security Program at CBRN Facilities, p.

Motivation also includes the "[threat] actor's belief that he possesses the necessary knowledge and capability to successfully carry out [an attack]" [53,54] whereas capability refers to the threat actor's actual capabilities relative to an organization's vulnerability to attack (i.e., opportunity in a broader context). We subsequently specify motivation, M, and capability, C, as potential attenuation factors, AF, for ARO.

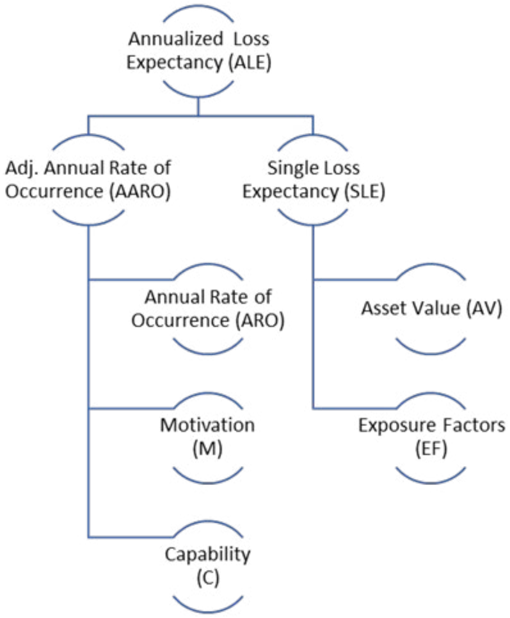

Annualized Loss Expectancy (ALE)
Adj. Annual Rate of Occurrence (AARO)
Single Loss Expectancy (SLE)
Annual Rate of Occurrence (ARO)
Asset Value (AV)
Motivation (M)
Exposure Factors (EF)
Capability (C)

Figure 18. Threat Actor Motivation and Capability in the ALE Model

We also note threat actor motivation and capability are impacted by other factors—not the least of which is an organization's security controls—and modify the model further to reflect correct placement of these factors.

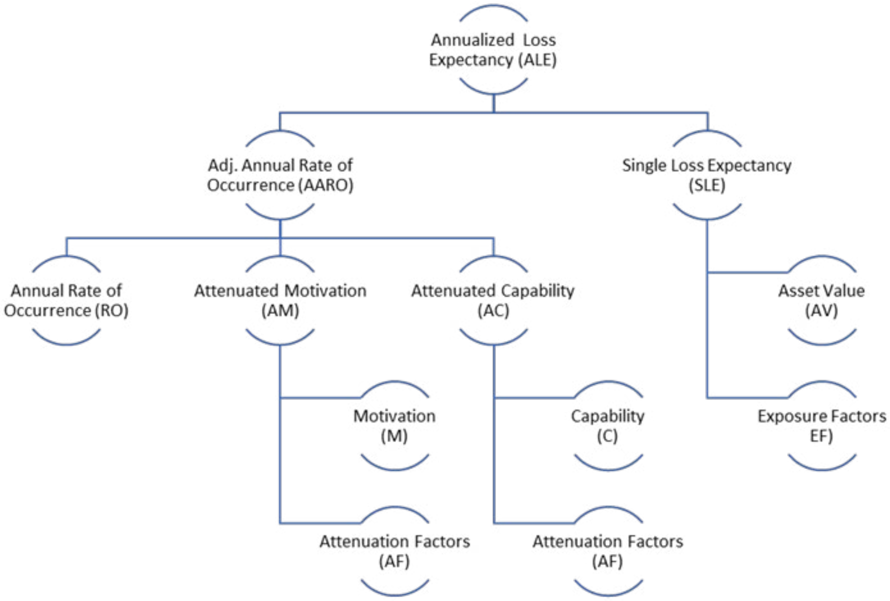

Annualized Loss Expectancy (ALE)
Adj. Annual Rate of Occurrence (AARO)
Single Loss Expectancy (SLE)
Annual Rate of Occurrence (RO)
Attenuated Motivation (AM)
Attenuated Capability (AC)
Asset Value (AV)
Motivation (M)
Capability (C)
Exposure Factors EF)
Attenuation Factors (AF)
Attenuation Factors (AF)

Figure 19. Modifying Motivation and Capability to Attenuate ARO in the ALE Model

[53] Wasson, J. and Bluesteen, C. (2017, Apr). Cognitive Defense: Influencing the Target Choices of Less Sophisticated Threat Actors. In Homeland Security Affairs (13), p. 5.

[54] The authors refer to this as opportunity as well; however, we choose to use the definition provided by CBRN Centres of Excellence (2015, Dec).

This model can now be modified to convert rates of occurrence—expressed as frequencies—to probabilities based on a time period in which less than ten (10) events occur. Our rationale is provided later when we present the frequency and probability tables.

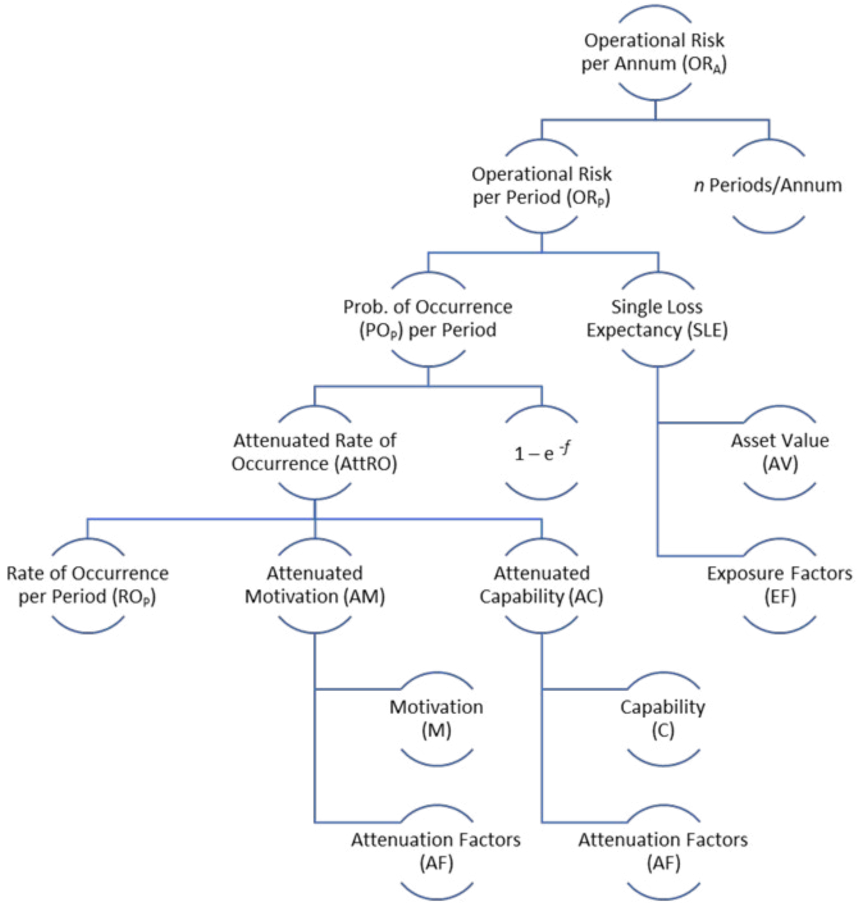

Operational Risk per Annum (OR_A)
Operational Risk per Period (OR_P)
n Periods/Annum
Prob. of Occurrence (PO_P) per Period
Single Loss Expectancy (SLE)
Attenuated Rate of Occurrence (AttRO)
$1 - e^{-f}$
Asset Value (AV)
Rate of Occurrence per Period (RO_P)
Attenuated Motivation (AM)
Attenuated Capability (AC)
Exposure Factors (EF)
Motivation (M)
Capability (C)
Attenuation Factors (AF)
Attenuation Factors (AF)

Figure 20. Incorporating Probability into the ALE Model

We then update the model to reflect per period rates of occurrence, RO_p prior to the probability conversion. By using a Poisson distribution with a mean equal to the frequency, f, we can estimate the probability of at least one (1) event in the time period, p, as $1 – e^{-f}$. The operational risk per period, OR_p is then computed as the probability of occurrence per period, PO_p multiplied by the single loss expectancy, SLE. Assuming each time period, pi, is statistically independent of any other of the n time periods, risk on an annual basis can then be computed as the product of the operational risk per period, OR_p and the number of periods, n.

All that remains to complete the computation model is adding the appropriate attenuation and exposure factors, which are the controls with functions relevant to the term being modified. Using our risk decomposition model:

- Motivation: deterrent controls
- Capability: preventive controls
- Asset value: detective, responsive, and recovery controls

To modify these terms, we note that control maturity scores must first be converted to a value between zero (0) and one (1), and the result must then be subtracted from one (1) since control maturity has an inverse relationship with motivation, capability, and asset value. In other words, as control maturity increases, the values for motivation, capability, and asset value—i.e., the loss in value—decreases.

The final computation model for direct opportunity risk is provided below. Note also that we replace the term, asset value or AV, with maximum loss, ML.

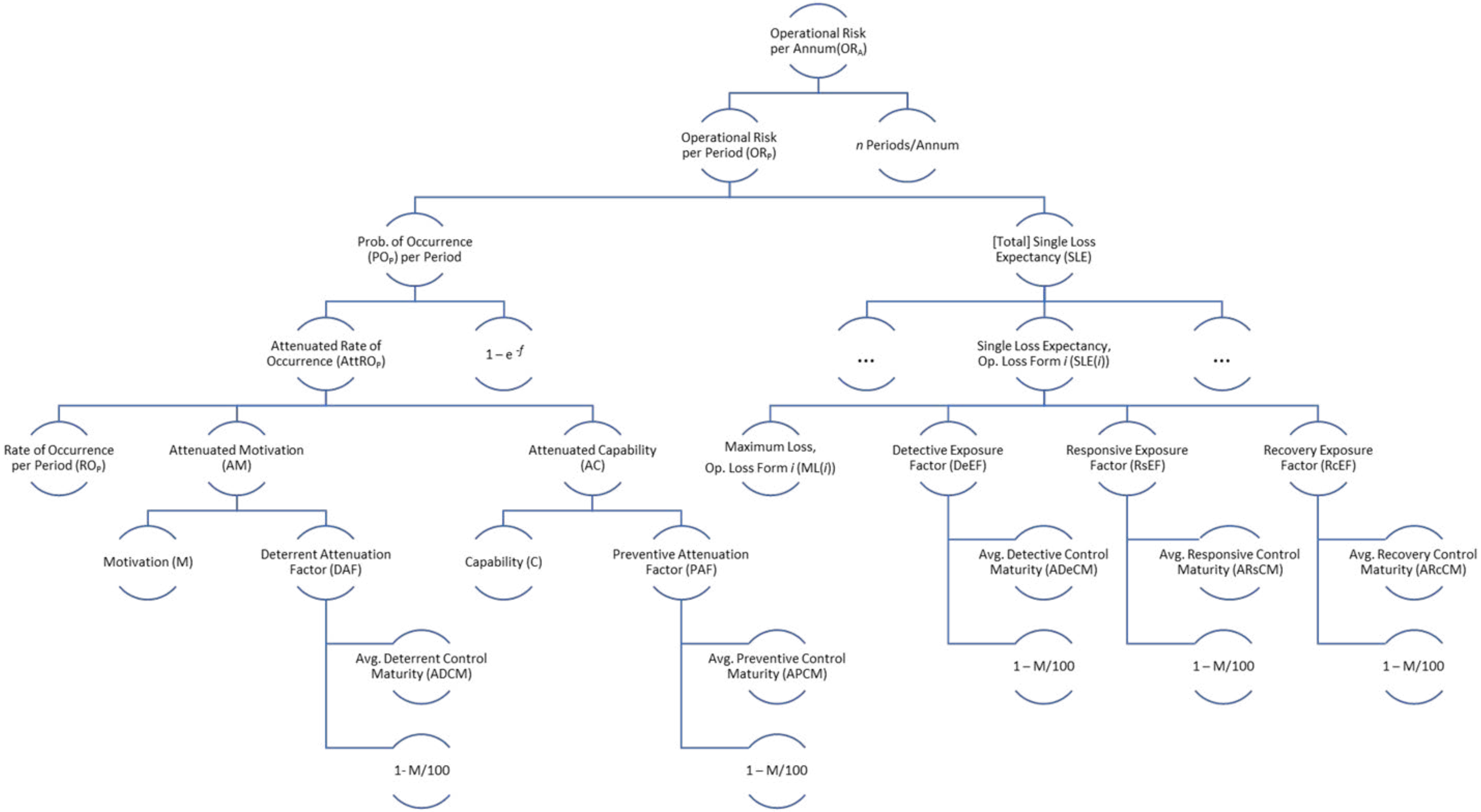

Operational Risk per Annum(OR$_A$)
Operational Risk per Period (OR$_P$)
n Periods/Annum
Prob. of Occurrence (PO$_P$) per Period
[Total] Single Loss Expectancy (SLE)
Attenuated Rate of Occurrence (AttRO$_P$)
$1 - e^{-f}$
…
Single Loss Expectancy, Op. Loss Form i (SLE(i))
…
Rate of Occurrence per Period (RO$_P$)
Attenuated Motivation (AM)
Attenuated Capability (AC)
Maximum Loss, Op. Loss Form i (ML(i))
Detective Exposure Factor (DeEF)
Responsive Exposure Factor (RsEF)
Recovery Exposure Factor (RcEF)
Motivation (M)
Deterrent Attenuation Factor (DAF)
Capability (C)
Preventive Attenuation Factor (PAF)
Avg. Detective Control Maturity (ADeCM)
Avg. Responsive Control Maturity (ARsCM)
Avg. Recovery Control Maturity (ARcCM)
Avg. Deterrent Control Maturity (ADCM)
Avg. Preventive Control Maturity (APCM)
1 – M/100
1 – M/100
1 – M/100
1- M/100
1 – M/100

Figure 21. QQRRA Operational (Direct) Risk Computation Model

Total operational risk, OR, is based on an evaluation of four separate categories of operational loss, SLE(i), that are directly attributable to a specific form of loss relevant to the threat event. Examples include but are not necessarily limited to lost revenue, LR, response cost(s), *RsC*, and recovery cost(s), *RcC*.[55] Estimates of relevant costs must be determined based on the information available to the risk analyst, and these costs are then adjusted based on the average maturity of relevant detective, responsive, and recovery controls: DeCM, RsCM, and RcCM, respectively.

Non-operational (Indirect) Risk

We now present our computation model for non-operational forms of risk.

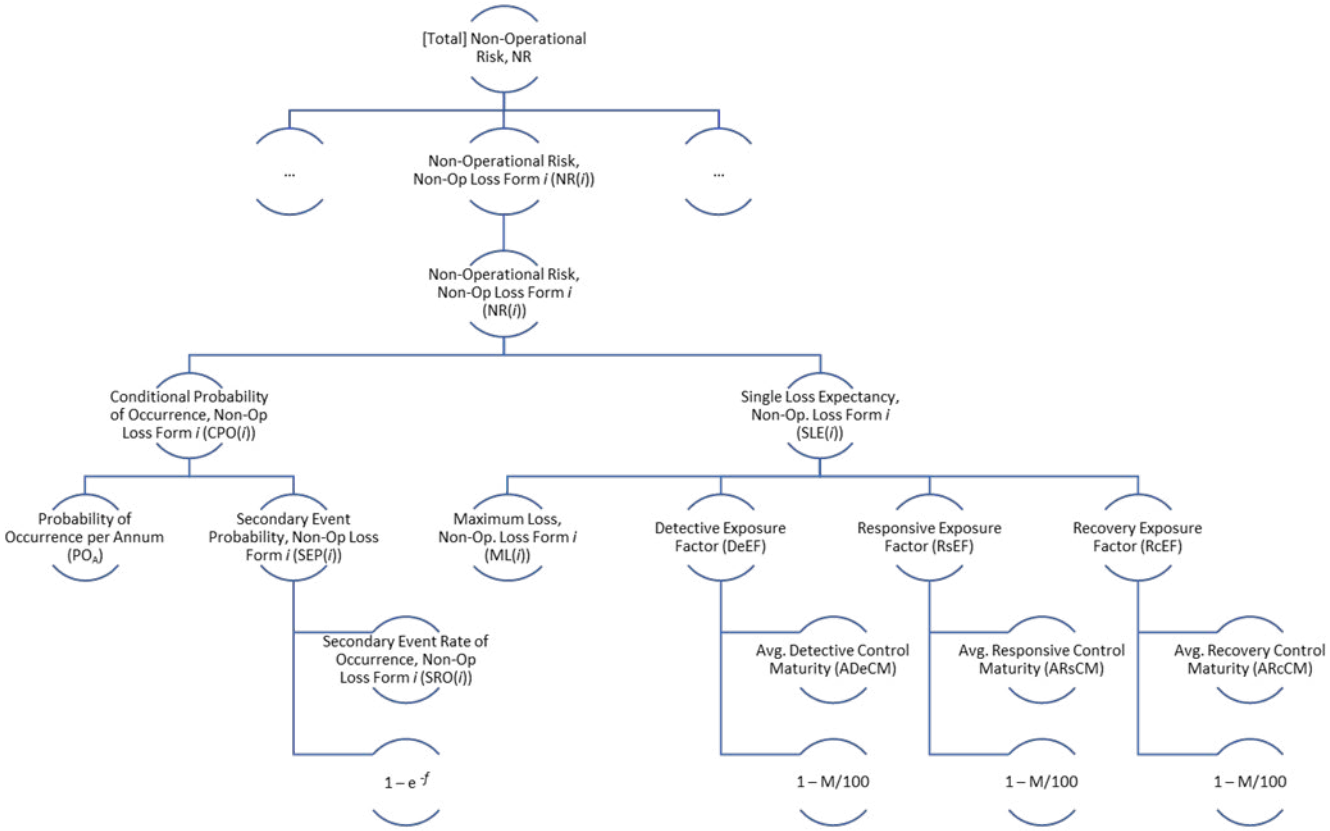

[Total] Non-Operational Risk, NR
...
Non-Operational Risk, Non-Op Loss Form *i* (NR(*i*))
...
Non-Operational Risk, Non-Op Loss Form *i* (NR(*i*))
Conditional Probability of Occurrence, Non-Op Loss Form *i* (CPO(*i*))
Single Loss Expectancy, Non-Op. Loss Form *i* (SLE(*i*))
Probability of Occurrence per Annum (PO$_A$)
Secondary Event Probability, Non-Op Loss Form *i* (SEP(*i*))
Maximum Loss, Non-Op. Loss Form *i* (ML(*i*))
Detective Exposure Factor (DeEF)
Responsive Exposure Factor (RsEF)
Recovery Exposure Factor (RcEF)
Secondary Event Rate of Occurrence, Non-Op Loss Form *i* (SRO(*i*))
Avg. Detective Control Maturity (ADeCM)
Avg. Responsive Control Maturity (ARsCM)
Avg. Recovery Control Maturity (ARcCM)
$1 - e^{-f}$
1 – M/100
1 – M/100
1 – M/100

Figure 22. QQRRA Non-operational (Indirect) Risk Computation Model

This model differs from the operational risk model in two important respects. First, probability of the second threat event occurring is conditioned on the probability the first event occurs. And second, risk is calculated separately for each form of indirect loss, i, as the conditional probability for each form could be different. For example, the probability a business partner or similar stakeholder might sue due to a breach of their customer's personal information would likely be different from the probability a regulator will impose fines or other penalties due to the breach.

[55] For example, see Forrester (2019, Aug). The Real Costs of Planned and Unplanned Downtime: Accelerate Recovery with New Technologies (Report).

The Calculus

Assumptions

A control specification, if based on a valid approach to risk analysis and properly applied, mitigates risk consistent with the organization's risk appetite. Further:

- The specified controls establish the organization's target profile
- The target profile establishes the organization's risk target

Full implementation of specified control requirements mitigates excessive residual risk to near zero, and residual risk within the organization's specified risk tolerance is considered acceptable.

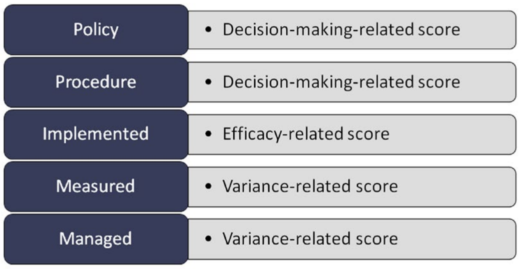
Each control requirement can be assessed for control efficacy, and efficacy can be determined by evaluating the maturity of its implementation in the intended environment.

The HITRUST control implementation maturity model provides a robust estimate of control efficacy (effectiveness), i.e., whether a control requirement:

- Is implemented,
- Is operating correctly (effectively), and
- Will continue to operate effectively in the future.

Each control requirement may be classified by its control function(s) (i.e., how it addresses a threat and associated risk).

As indicated in the figure below, maturity levels for policy and procedure, evaluated in the broader context of related decision support controls, will provide better estimates of control efficacy. Similarly, maturity levels for measured and managed, evaluated in the broader context of related variance reduction controls, will also provide better estimates of control efficacy.



Policy	• Decision-making-related score
Procedure	• Decision-making-related score
Implemented	• Efficacy-related score
Measured	• Variance-related score
Managed	• Variance-related score

Figure 23. Applying Decision Support and Variance Reduction Controls to the Implementation Maturity Model

Maturity scores for control requirements aggregated by control function can be used to estimate how they mitigate the risk posed by related threats.

General Approach

QQRRA is designed to evaluate levels of residual risk without the need for a comprehensive quantitative risk analysis of inherent risk—either broadly in terms of the organization's overall risk profile or more narrowly in terms of a specific type of inherent risk (e.g., from using cloud services)—by leveraging the concept of control framework-based risk analysis. In other words, it relies on the initial risk analysis done by a standards body such as NIST and the additional tailoring required to complete the analysis and specify a reasonable and appropriate set of controls that will provide adequate protection of one's sensitive information.

QQRRA is based on performing multiple contextual analyses such as a 'baseline' analysis to estimate unknown parameters in the model and subsequent analyses based on the organization's Current ('as is') and Target ('to be') profiles.[56]

A baseline analysis is performed to create a risk estimate that assumes the average maturity scores of relevant information security controls for organizations that are 'typically' subject to the threats/risks that are the focus of the analysis. Assumptions of average control maturity are based on data available from the HITRUST Assurance Program, HITRUST Organizations, and HITRUST External Assessors. The intent is to integrate information about these risks, which may be available publicly or internally to the organization, into the analysis and then adjust one's estimates of those risks in further contextual analyses based on the current or future (intended or target) state of the organization's controls.

It is also possible to compare scores from an organization's Current Profile with its Target Profile to evaluate risk reduction from addressing control deficiencies.

Risk Tables

Although we present a computation model that leverages quantitative tables to aid in estimation, empirical estimates for these parameters may also be used when such information is available (e.g., from actuarial tables and security surveys, reports, and studies). They can be used directly to populate parameters in the analysis or indirectly as a means of identifying an appropriate category (or categories) from one of the quasi-quantitative tables used in the analysis.

Note risk tables used for non-frequency parameters in the QQRRA approach are similar to those used by NIST; however, their tables tend to follow a normal distribution with a wide range of values (percentages or probabilities) around the middle or average. For example, 'moderate' in the NIST approach addresses between 21% and 79% of a population parameter.[57]

We subsequently modify the NIST approach by providing additional granularity for this broad middle range, as shown in the following table, and use it whenever there is an assumption of normality for the parameter being evaluated.

Table 1. Measurement Scales

Qualitative Scale	Quasi-Quantitative Scales		Quantitative Scales	
	10-Point Scale	Fibonacci Scale	Midpoint	% / Probability
Very High	10	13	98	96-100
High	9	8	87	80-95
Above Average	7	5	70	60-79
Average	5	3	50	40-59
Below Average	3	2	30	20-39
Low	1	1	13	5-20
Very Low	0	0	2	0-4

Frequency (f)

Probability based on frequency approaches '1' exponentially after a frequency of '10'. QQRRA addresses this problem by limiting the period of analysis in which the event occurs so that future conversion from frequency to probability remains meaningful. For example, an occurrence of 365 times per year would be converted to one occurrence per day, the analysis would be performed for that 1-day period, and—based on an assumption of independence of occurrence between time periods—the risk calculation would be adjusted to span the entire year.

[56] NIST (2018, 16 Apr).

[57] For example, see JTF TI (2012, Sep). Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1). Gaithersburg, MD: NIST, p. F-2.

<< Back to Contents

Table 2. Relationship Between Frequency and Probability

Frequency	Probability	Qualitative Rating
>1	0.63 - ~1.0	Plentiful
0.7 – 1	0.5 – 0.63	Common
0.36 – 0.7	0.3 – 0.5	Not Uncommon
0.23 – 0.36	0.2 – 0.3	Moderately Uncommon
0.11 – 0.23	0.1 – 0.2	Uncommon
0.01 – 0.1 (10^{-2} – 10^{-1})	0.01 – 0.1 (10^{-2} – 10^{-1})	Somewhat Rare
0.001 – 0.01 (10^{-3} – 10^{-2})	0.001 – 0.01 (10^{-3} – 10^{-2})	Moderately Rare
0.0001 – 0.001 (10^{-4} – 10^{-3})	0.0001 – 0.001 (10^{-4} – 10^{-3})	Rare
0.00001 – 0.0001 (10^{-5} – 10^{-4})	0.00001 – 0.0001 (10^{-5} – 10^{-4})	Very Rare
0.000001 – 0.00001 (10^{-6} – 10^{-5})	0.000001 – 0.00001 (10^{-6} – 10^{-5})	Extremely Rare
Unless data is available, lower values should not be used		Extraordinarily Rare

Table 2 depicts the relationship between frequency and probability as well as how a particular range of frequencies or probabilities may be described qualitatively, and examples of how one can interpret these frequencies based on real world examples are provided in the following two tables.[58]

Table 3. Real World Examples of Frequency and Probability Categories

Qualitative Scale	Description	Example 1	Example 2	Frequency	Probability
Plentiful	Usually, almost always	At least one sunny weekend in the next year	Finding at least one container of ice cream in a family freezer	> 1	0.63 - ~1.0
Common	Common, must be considered, not always	Getting stuck in a traffic jam for at least 20 minutes next year (exclude commuting)	A member of the family gets a cold next year	0.7 – 1	0.5 – 0.63
Not Uncommon	Not uncommon	That a person between the age of 18 and 29 does NOT read a newspaper regularly	Divorcing, depending on the country (reportedly 30-40%)	0.36 – 0.7	0.3 – 0.5
Moderately Uncommon	Maybe, possibly	A celebrity marriage will last a lifetime	Stuck in traffic for more than 1 hour (exclude commuting)	0.23 – 0.36	0.2 – 0.3
Uncommon	Not usually, occasionally	Chance of drawing 1 when drawing a fair dice (1/6=0.16)	Mortality rate of SARS (11%) of people diagnosed with the disease	0.11 – 0.23	0.1 – 0.2
Rare	Rarely, almost never, never	A non-expert should stop here at this level of scrutiny. Experts can develop more in-depth estimates for lower probabilities levels using the next table below.			0 – 0.1

[58] Adapted from Riskope (2017, Feb 1). Making Sense of Probabilities and Frequencies.

Table 4. Real World Examples of Frequency and Probability Categories (Rare)

Qualitative Scale	Likelihood of 'Rare" Phenomena	Example 1	Example 2	Return Time (Yrs) Prob≈Freq	Probability
Somewhat Rare	High	Being born a twin (3.3%), drawing an ace from a 52-card deck (7.7%)	Higher bound of likelihood to have a >7.0 magnitude quake on the San Andreas Fault	100 – 10	0.01 – 0.1 (10-^{2} – 10-^{1})
Moderately Rare	Moderate	Being a millionaire in the U.S. (≈0.9%)	Drunken pilot on a plane (1.2/1000)	1,000 – 100	0.001 – 0.01 (10-^{3} – 10-^{2})
Rare	Low	Rate of centenarians (1.7 to 3.4 per 10,000 based on country of birth)	An earth tailings dam breach	10K – 1000	0.0001 – 0.001
Very Rare	Very Low	Injury from fireworks	Class 5+ nuclear accident	100K – 10K	0.00001 – 0.0001 (10-^{5} – 10-^{4})
Extremely Rare	Extremely Low	Being a billionaire in the U.S. (≈1/780,000)	Stricken by lightning (similar to column on the right)	1M – 100K	0.000001 – 0.00001 (10-^{6} – 10-^{5})
Extraordinarily Rare	Credibility Threshold	Winning $200M in the National Lottery	Meteor landing precisely on your house; a major Swiss hydro-dam breaching	N/A	Unless data is available, lower values should not be used

Motivation

Threat actor motivation, M, is formally defined as the likelihood a threat agent will initiate a threat action and is assumed to be normally distributed. For the sake of simplicity, we only include qualitative descriptors in the table that follows. Motivation can also be dependent on other factors, such as the type of organization (e.g., an oil company or national defense contractor) or information (e.g., payment card data or health records) being targeted. Motivation for a threat actor may therefore differ from one analysis to the next.

Table 5. Motivation Scale

Quantitative Scale (Midpoint)	Motivation Description
98%	• Extreme drive or purpose for exploitation of an opportunity, and will attempt to exploit an opportunity more than 96% of the time • Examples include but are not limited to extremists or nation-state actors, organized crime/ cybercriminals, hacktivist groups
87%	• Highly driven or has an express purpose for exploitation of an opportunity, and will attempt to exploit an opportunity between 80% and 95% of the time • Examples include but are not limited to lone criminals, individual hacktivists
70%	• Has an above average drive or purpose for exploitation of an opportunity, and will attempt to exploit an opportunity between 60% and 79% of the time • Examples include but are not limited to disgruntled users/insiders
50%	• Moderate or average drive or purpose for exploitation of an opportunity, and will attempt to exploit an opportunity between 40% and 59% of the time • Examples include but not limited to hackers looking for targets of opportunity to support other attacks
30%	• Below average drive or purpose for exploitation of an opportunity, and will only attempt to exploit an opportunity between 20% and 39% of the time • Examples include but are not limited to hackers simply seeking chaos and destruction
13%	• Low drive or purpose for exploitation of an opportunity, and will only attempt to exploit an opportunity between 5% and 19% of the time • Examples include but are not limited to opportunistic users/insiders, script kiddies
2%	• Little to no drive or purpose for exploitation of an opportunity, and will only attempt to exploit an opportunity less than 4% of the time • Examples include but are not limited to non-malicious users/insiders

Capability (C)

A threat actor's capability, C, may be assessed individually or as a function of its two primary components: skills, S, and resources, R, as shown in the three tables that follow.

Table 6. Capability

Quantitative Scale (Midpoint)	Capability Description
98%	• Highly capable; capable of exploiting related vulnerabilities and successfully initiating a threat event more than 96% of the time • Examples include but are not limited to nation states
87%	• Very capable; capable of exploiting related vulnerabilities and successfully initiating a threat event between 80% to 95% of the time • Examples include but are not limited to organized crime
70%	• Above average capability; capable of exploiting related vulnerabilities and successfully initiating a threat event between 60% and 79% of the time • Examples include but are not limited to hacktivist organizations
50%	• Moderate capability; capable of exploiting related vulnerabilities and successfully initiating a threat event between 40% to 59% of the time • Examples include but are not limited to a typical hacker
30%	• Below average capability; capable of exploiting related vulnerabilities and successfully initiating a threat event between 20% to 39% of the time • Examples include but are not limited to a typical disgruntled employee
13%	• Limited capability; capable of exploiting related vulnerabilities and successfully initiating a threat event between 5% to 19% of the time • Examples include but are not limited to script kiddies
2%	• Little to no capability; capable of exploiting related vulnerabilities and successfully initiating a threat event less than 4% of the time • Examples include but are not limited to non-malicious users/insiders

Table 7. Skills

Quantitative Scale (Midpoint)	Skill Description
98%	• Highly skilled and comprehensively trained with respect to related threats; top 96% of all threat actors • Examples include but are not limited to nation states
87%	• Very skilled and trained with respect to related threats; top 80% to 95% of all threat actors • Examples include but are not limited to organized crime
70%	• Above average skill and training with respect to related threats; top 60% to 79% of all threat actors • Examples include but are not limited to hacktivist organizations
50%	• Moderate skill and training with respect to related threats; average 40% to 59% of all threat actors • Examples include but are not limited to typical hacker
30%	• Below average skill and training with respect to related threats; bottom 20 to 39% of all threat actors • Examples include but are not limited to disgruntled employees
13%	• Limited knowledge and training with respect to related threats; bottom 5% to 19% of all threat actors • Examples include but are not limited to script kiddies
2%	• No knowledge or training with respect to related threats; bottom 4% of all threat actors • Examples include but are not limited to non-malicious users/insiders

Table 8. Resources

Quantitative Scale (Midpoint)	Resource Description
98%	• Fully resourced and funded with respect to related threats; top 96% of all threat actors • Examples include but are not limited to nation states
87%	• Significant resources and funding with respect to related threats; top 80% to 95% of all threat actors • Examples include but are not limited to organized crime
70%	• Above avg. resources and funding with respect to related threats; top 60% to 79% of all threat actors • Examples include but are not limited to hacktivist organizations
50%	• Moderate resources and funding with respect to related threats; avg. 40% to 59% of all threat actors • Examples include but are not limited to small/ad hoc groups of threat actors
30%	• Below avg. resources and funding with respect to related threats; bottom 20% to 39% of all actors • Examples include but are not limited to individual threat actors
13%	• Limited resources and funding with respect to related threats; bottom 5% to 19% of all threat actors • Examples include but are not limited to script kiddies
2%	• Few if any resources and funding with respect to related threats; bottom 4% of all threat actors • Examples include but are not limited to non-malicious users/insiders

We now turn to the table required to estimate the conditional probability of occurrence, CPO, of a non-operational threat, which would be initiated by a stakeholder such as regulator, when an operational loss event occurs.

Table 9. Secondary Event Probability

Quantitative Scale (Midpoint)	SEP Description
98%	• Very high response rate; responds to similar loss events more than 96% of the time
87%	• High response rate; responds to similar loss events between 80% to 95% of the time
70%	• Above avg. response rate; responds to similar loss events between 60% to 79% of the time
50%	• Avg. response rate; responds to similar loss events between 40% to 59% of the time
30%	• Below avg. response rate; responds to similar loss events between 20% to 39% of the time
13%	• Low response rate; responds to similar loss events between 5% to 19% of the time
2%	• Very low response rate; responds to similar loss events less than 4% of the time

(Maximum) Loss

Costs (loss) should always be estimated directly or indirectly based on empirical data. For example, the replacement cost of a physical asset can almost always be determined directly. However, some costs like fines and other penalties due to regulatory non-compliance may not be as straightforward. In this case, available information on previous fines and other penalties levied by the relevant regulator(s) may be used to estimate maximum, most likely, and minimum loss values or help select a range of loss from a quasi-quantitative table of potential losses.

If loss tables are used to help guide an organization's estimate of potential loss magnitude, QQRRA accommodates an approach that can be tailored to an organization based on an estimate of its risk capacity, RCap, i.e., the maximum level of risk that a firm can absorb financially and remain solvent. For our purposes, we compute RCap as the sum of the organization's available cash and cash equivalents, marketable securities, and accounts receivable less its current liabilities, and then use this value to help 'cap' the tables and assign each category's quasi-quantitative lower and upper bounds.

Table 10. Impact Categories and Quantitative Scales

Qualitative Scale	% of RCap	
	Lower Bound	Upper Bound
Extraordinarily Catastrophic	67.65%	109.46% (∞)
Extremely Catastrophic	41.81%	67.65%
Very Catastrophic	25.84%	41.81%
Catastrophic	15.97%	25.84%
Extremely Severe	9.87%	15.97%
Very Severe	6.1%	9.87%
Severe	3.77%	6.1%
Extremely Significant	2.33%	3.77%
Very Significant	1.44%	2.33%
Significant	0.89%	1.44%
Extremely Major	0.55%	0.89%
Very Major	0.34%	0.55%
Major	0.21%	0.34%
Moderate	0.13%	0.21%
Minor	0.08%	0.13%
Very Minor	0.05%	0.08%
Minimal	0.03%	0.05%
Very Minimal	0.02%	0.03%
Negligible	0.01%	0.02%
Very Negligible	0%	0.01%

Note the lowest level of loss magnitude has the smallest range, and the range of each category gets progressively larger as one approaches RCap. Basing the quasi-quantitative ranges on a Fibonacci sequence allows for higher granularity when losses are perceived to be small but still allows a relatively limited number of quasi-quantitative categories to address the exceedingly broad range between zero loss and the maximum loss an organization can endure and remain solvent.

It is also important to note that, since the table uses RCap to provide a 'maximum' value or 'cap' for loss, it can also be used to express individual risks as well as the organization's total risk exposure in qualitative terms that is contextual to the organization. The quasi-quantitative ranges—and especially the mid-points we will use in our risk calculations—will in turn allow risk information to be conveyed in a standardized way across all organizations.

To illustrate what this might look like for a specific company, assume RCap is $10M. The table this organization would use to categorize loss (or risk) would subsequently appear as shown in Table 11.

Table 11. Contextual Example of Impact Categories and Scales

Qualitative Scale	% of RCap	
	Lower Bound	Upper Bound
Extraordinarily Catastrophic	$6.765M	$10.946M (∞)
Extremely Catastrophic	$4.181M	$6.765M
Very Catastrophic	$2.584M	$4.181M
Catastrophic	$1.597M	$2.584M
Extremely Severe	$987K	$1.597M
Very Severe	$610K	$987K
Severe	$377K	$610K
Extremely Significant	$233K	$377K
Very Significant	$144K	$233K
Significant	$89K	$144K
Extremely Major	$55K	$89K
Very Major	$34K	$55K
Major	$21K	$34K
Moderate	$13K	$21K
Minor	$8K	$13K
Very Minor	$5K	$8K
Minimal	$3K	$5K
Very Minimal	$2K	$3K
Negligible	$1K	$2K
Very Negligible	$0	$1K

Worked Example

In this example, we wish to evaluate the risk associated with the threat of ransomware, i.e., making the organization's data inaccessible unless and until a monetary ransom is paid to a threat actor. The relevant threat in the HITRUST Threat Catalogue is LIN32 – Logical Threats: Intentional: Nefarious: Ransomware, which is defined as "infection of a computer system or device by malware that restricts access to the system and information while demanding that the user pays a ransom to remove the restriction."

We assume control requirements relevant to the threats have been obtained from a reliable source such as the HITRUST CSF, control functions have been assigned to each control requirement, and scores for each maturity level are available from either internal or external assessment.

Contextual Analysis - Baseline

For simplicity, we assume the maturity scores for an average organization are uniform across all controls and adjust (1) the policy and procedure scores by the average score for all decision support controls and (2) the measured and managed scores by the average score for all variance reduction controls related to the ransomware threat.

Table 12. Example HITRUST Assessment Results (Baseline Analysis)

Maturity Level	Level of Compliance	Score
Policy	50%	7.50
Procedure	50%	10.00
Implemented	75%	30.00
Measured	50%	5.00
Managed	0%	0.00
Total	-	52.50
Policy (Adjusted)	-	3.94
Procedure (Adjusted)	-	5.25
Implemented	-	30.00
Measured (Adjusted)	-	2.63
Managed (Adjusted)	-	0.00
Total (Adjusted)	-	41.81

The adjustments are computed by multiplying each maturity level for a control by the average total maturity score of relevant decision support and variance reduction controls expressed as a percentage. Alternatively, one could adjust the scores by computing simple averages.

Calculating Operational (Direct) Risk

To compute the annualized operational risk, OR_A, for the baseline analysis, we will take a 'bottom up' approach starting with the rate of occurrence calculations and then moving on to the total single loss expectancy, SLE.

According to a 2021 survey,[59] about 51% of companies in the United States that participated in the survey stated they experienced a ransomware attack in the past year.[60] Since this observed rate/frequency is less than one (1), the number of periods per annum, n, is one (1), and the attenuated rate of occurrence per annum, $AttRO_A$, is estimated at 0.51 times per year

$$AttRO_A = 0.51$$

Before calculating the probability of occurrence per annum, PO_A, we will 'reverse engineer' the rate of occurrence per annum, RO_A, as this value is needed for further contextual analysis against the organization's Current or Target Profiles.

To do this, we assume the threat actor in this scenario is organized crime. This yields a motivation, M, of 0.98, and a capability, C, of 0.87. We subsequently estimate AM and AC as follows.

$$AM = M \cdot (1 - ADCM/100) = (0.98)\ (1 - 41.81/100) = (0.98)\ (0.5819) \approx 0.5703$$

$$CM = C \cdot (1 - APCM/100) = (0.87)\ (1 - 41.81/100) = (0.87)\ (0.5819) \approx 0.5063$$

[59] Sophos (2021, Apr). The State of Ransomware 2021, p. 3.

[60] If specific data on attempted ransomware attacks on one's own company were available, we could either replace the survey frequency or take a Bayesian approach to modify this parameter based on the additional evidence.

It is now a simple matter computing ROA.

$$\mathrm{AttRO_A = RO_A \cdot AM \cdot CM}$$

$$\mathrm{RO_A = AttRO_A / (AM \cdot CM)}$$

$$\mathrm{RO_A} = (0.51) / [(0.5703)\ (0.5063)] \approx 0.51 / 0.2887 \approx 1.7665$$

The result suggests that, without the controls implemented at the maturity level of an 'average' or 'typical' organization, one would expect ransomware attacks to occur approximately 1.7 to 1.8 times per year.

We now estimate the probability of occurrence per annum, $\mathrm{PO_A}$.

$$\mathrm{PO_A} = 1 - e\ \text{-}f = 1 - e^{-\mathrm{AttRO}}{}_{\mathrm{A}} = 1 - e^{-0.51} \approx 1 - 0.6005 = 0.3995$$

To compute (total) single loss expectancy, SLE, we need to compute the expected loss from all relevant loss forms; however, for simplicity, we will focus on a single loss form, recovery cost or RcC, i.e., SLE(RcC).

There are several ways in which losses can be estimated, e.g., by reviewing research studies that address related loss events; directly calculating such losses based on what we know about our particular situation (such as how much data we actually have and the replacement cost of specific information assets), or using this information to modify estimates obtained from other sources in a Bayesian approach to determine the most probable loss (such as through Monte Carlo simulation). For the purpose of this exercise, we will take the first approach but include the caveat that additional research would be needed to ensure the best estimates applicable to a specific entity/situation.

For the purpose of this exercise, we will use an average cost of $1.85M for remediating a ransomware attack, SLE(RcC), based on the same survey[61] (again, assuming all other costs are zero for simplicity).

$$\mathrm{SLE = SLE(RcC)} = \$1.85\mathrm{M}$$

Again, as with the computation of the rate of occurrence per period, $\mathrm{RO_P}$, earlier, we need to 'reverse engineer' the value of maximum loss for the recovery loss form, ML(RcC). Since the control maturity scores are uniform for this example, we note that average maturity for all controls regardless of purpose is 41.81, and the resulting computations are fairly straightforward.

$$\mathrm{SLE(RcC) = ML(RcC) \cdot DeEF \cdot RsEF \cdot RcEF}$$

$$\mathrm{ML(RcC) = SLE(RcC) / (DeEF \cdot RsEF \cdot RcEF)}$$

$$\mathrm{ML(RcC) = SLE(RcC) / [(1 - DeCM/100)\ (1 - RsCM/100)\ (1 - RcCM/100)]}$$

$$\mathrm{ML(RcC)} = (\$1.85\mathrm{M}) / [(1 - 41.81/100)\ (1 - 41.81/100)\ (1 - 41.81/100)]$$

$$\mathrm{ML(RcC)} = (\$1.85\mathrm{M}) / [(0.5819)\ (0.5819)\ (0.5819)] = \$1.85\mathrm{M} / 0.1970 \approx \$9.3909\mathrm{M}$$

The result suggests that, without the controls implemented at the same maturity level as a 'typical' organization, one would expect ransomware attacks to cost approximately $9.39M on average.

[61] Sophos (2021, Apr).

We can now compute the operational risk per annum, ORA, directly from the probability of occurrence per annum, POA, and our (total) single loss expectancy, SLE.

$$OR_A = PO_A \cdot SLE = (0.3995)\ (\$1.85M) = \$0.7391M \text{ or } \$739.1K$$

Calculating Non-Operational (Indirect) Risk

Calculating non-operational risk, NR, is a bit easier than it is for operational risk as (1) there is no need to compute period and annual values since we condition a secondary event probability on the annual probability of occurrence of the initial threat event, PO_A and (2) we only need to 'reverse engineer' a single value as opposed to two values with operational risk. We also do not need to convert a rate of occurrence into a probability if we use our probability of occurrence table to estimate the probability. However, if we base it on an observed rate, one can use the same approach for the conversion as was used previously, i.e., compute $1 - e^{-f}$ and convert the result to per annum probability if the period, p, is less than annual.

For this example, we will limit our calculation of non-operational (indirect) risk, NR, to the compliance loss form, NR(Comp).

We will also assume the organization is a covered entity[62] subject to the Health Information Portability and Accountability Act (HIPAA)[63] Security Rule (HSR),[64] which is enforced by the Department of Health and Human Services (HHS)[65] Office of Civil Rights (OCR).[66] Given OCR has a demonstrable history of investigating significant breaches of electronic Protected Health Information, ePHI, such as those caused by ransomware, we can easily assign a secondary event probability for the compliance loss form, SEP(Comp) of 'moderately uncommon' to 'not uncommon.' Since we are straddling two categories, we can either take their common upper and lower bound of 0.30 or take the midpoint between the upper bound for 'not uncommon' and the lower bound of 'moderately uncommon,' which yields a value of 0.35. We select the latter approach for consistency.

We can now compute the conditional probability of occurrence for the compliance loss form, CPO(Comp).

$$CPO(Comp) = PO_A \cdot SEP(Comp) = 0.3995 \cdot 0.35 \approx 0.1398$$

Estimating the impact of non-operational (indirect) risk, NR, is essentially identical to operational loss forms, i.e., estimates are based on data available to the analyst conducting the risk assessment. For the purpose of this exercise, we will assume available data indicates the single loss expectancy for the compliance loss form would be $1M in fines, penalties, and other costs associated with a resolution agreement,[67] i.e.:

$$SLE(Comp) = \$1M$$

We will now 'reverse engineer' the maximum loss for compliance costs, ML(Comp), as we will need this later for contextual analysis based on the organization's current or target profile.

$$SLE(Comp) = ML(Comp) \cdot (1 - ADeCM/100)\ (1 - ARsCM/100)\ (1 - ARcCM/100)$$

$$ML(Comp) = SLE(Comp) / [(1 - DeCM/100)\ (1 - RsCM/100)\ (1 - RcCM/100)]$$

$$ML(Comp) = \$1M / [(1 - 41.81/100)\ (1 - 41.81/100)\ (1 - 41.81/100)]$$

[62] Health and Human Services, HHS (2022a). HIPAA: HIPAA Home: For Professionals: Covered Entities and Business Associates.

[63] HHS (2022b). HIPAA: HIPAA Home: HIPAA for Professionals.

[64] HHS (2022c). HHS: HIPAA Home: For Professionals: The Security Rule.

[65] HHS (2022d). Home: About HHS.

[66] HHS (2022e). HHS: OCR Home: About Us.

[67] HHS (2022f). HHS: HIPAA Home: For Professionals: HIPAA Compliance and Enforcement: Resolution Agreements.

$$ML(Comp) = \$1M / [(0.5819)\ (0.5819)\ (0.5819)]$$

$$ML(Comp) \approx \$1M / 0.1970$$

$$ML(Comp) \approx \$5.0761M$$

And finally, (total) non-operational (indirect) risk, NR, is estimated as follows:

$$NR = NR(Comp) = CPO(Comp) \cdot SLE(Comp) = (0.1398)\ (\$1M) = \$0.1398M = \$139.8K$$[68]

Calculating Total Risk

Total risk for the baseline context, R, is simply the sum of all operational (direct) and non-operational (indirect) risks, OR_A and *NR*, respectively.

$$R = OR_A + NR = \$739.1K + \$139.8K = \$878.9K$$

A total risk of $878.9K can be considered a very severe risk for an organization with an RCap of only $10M.

Contextual Analysis – Current Profile

In this scenario, we assume the following about the current state of the organization's information security controls, i.e., its Current Profile.

Table 13. Example HITRUST Assessment Results (Contextual Analysis)

Maturity Level	Level of Compliance	Score
Policy	100%	15.00
Procedure	50%	10.00
Implemented	100%	40.00
Measured	50%	5.00
Managed	50%	7.50
Total	-	77.50
Policy (Adjusted)	-	11.63
Procedure (Adjusted)	-	7.75
Implemented	-	40.00
Measured (Adjusted)	-	3.88
Managed (Adjusted)	-	5.81
Total (Adjusted)	-	69.06

As before, the adjustments are computed by multiplying each maturity level for a control by the average total maturity score of relevant decision support and variance reduction controls expressed as percentage.

[68] If a cyber insurance policy covers related costs, then the amount that would be paid by the insurer would necessarily be discounted.

Calculating Operational (Direct) Risk

We now compute the operational (direct) risk, OR_A, associated with the organization's Current Profile. We first calculate a new value for the attenuated rate of occurrence per annum $AttRO_A$.

$$AttRO_A = RO_A \cdot AM \cdot CM$$

$$AttRO_A = RO_A \cdot [(M \cdot (1 – ADCM/100)) \cdot (C \cdot (1 – APCM/100))]$$

$$AttRO_A = (1.7665)\ [(.98)\ (1 – 69.06/100)]\ [(.87)\ (1 – 69.06/100)]$$

$$AttRO_A = (1.7665)\ [(.98)\ (0.3094)]\ [(.87)\ (0.3094)]$$

$$AttRO_A \approx (1.7665)\ (0.3032)\ (0.2692) \approx 0.1442$$

We can now estimate the probability of occurrence per annum, PO_A.

$$PO_A = 1 – e\ \text{-}f = 1 – e^{-ATTRO_A} = 1 – e^{-\,0.1442} \approx 1 – 0.8657 = 0.1343$$

The (total) single loss expectancy, SLE, can be calculated from the expected loss from the payment of ransomware as the sole recovery cost, SLE(RcC).

$$SLE = SLE(RcC) = ML(RcC) \cdot DeEF \cdot RsEF \cdot RcEF$$

$$SLE = ML(RcC)\ (1 – DeCM/100)\ (1 – RsCM/100)\ (1 – RcCM/100)$$

$$SLE = (\$9.3909)\ (1 – 69.06/100)\ (1 – 69.06/100)\ (1 – 69.06/100)$$

$$SLE = (\$9.3909M)\ (0.3094)\ (0.3094)\ (0.3094) \approx \$0.2781M \approx \$278.1K$$

And finally, the operational risk per annum, OR_A, is computed as follows.

$$OR_A = PO_A \cdot SLE = (0.1343)\ (\$278.1K) \approx \$37.3488K \approx \$37.3K$$

Calculating Non-Operational (Indirect) Risk

As before, we limit our calculation of non-operational (indirect) risk, NR, to the compliance loss form, NR(Comp), and use the same healthcare compliance scenario.

We can now compute the conditional probability of occurrence for the compliance loss form, CPO(Comp).

$$CPO(Comp) = PO_A \cdot SEP(Comp) = 0.1343 \cdot 0.35 \approx 0.0470$$

We will now derive single loss expectancy for the compliance loss form, SLE(Comp), from the loss form's maximum loss, ML(Comp).

$$SLE(Comp) = ML(Comp) \cdot (1 – ADeCM/100)\ (1 – ARsCM/100)\ (1 – ARcCM/100)$$

$$SLE(Comp) = (\$5.0761M)\ [(1 – 69.06/100)\ (1 – 69.06/100)\ (1 – 69.06/100)]$$

$$SLE(Comp) = (\$5.0761M)\ (0.3094)\ (0.3094)\ (0.3094) \approx \$0.1503M = \$150.3K$$

And finally, (total) non-operational (indirect) risk, NR, is estimated as follows:

$$NR = NR(Comp) = CPO(Comp) \cdot SLE(Comp) = (0.0470)\ (\$150.3K) \approx \$7.0651K \approx \$7.1K$$

Calculating Total Risk

Total risk for the baseline context, R, is simply the sum of all operational (direct) and non-operational (indirect) risks, OR_A and *NR*, respectively.

$$R = OR_A + NR = \$37.3K + \$7.1K = \$44.4K$$

$44.4K would be considered a very major risk for an organization with an RCap of only $10M.

Calculating Risk Reduction

We can now compute the ransomware risk reduction between an organization with an 'average' information security program represented by its control maturity scores and the organization conducting the risk analysis that has a more mature program

Table 14. Risk Reduction (Compared to Baseline)

Risk	Baseline	Current Profile	Difference	% Reduction
Operational	$739.1K	$37.3K	$701.8K	95.0%
Non-Operational	$139.8K	$7.1K	$132.7K	94.9%
Total	$878.9K	$44.4K	$834.5K	95.0%

Flexibility of Approach

The HITRUST patent pending QQRRA approach can be adapted to virtually any type of analysis, whether it addresses one or multiple risks or controls. It can use a 'typical' or 'average' organization as a baseline of comparison with its current state (current profile), or it can be used to assess the differences between one's current and future state (target profile) for one or more controls. Simple analyses can be performed in a spreadsheet, or more complex analysis with a many-to-many mapping between threats/risks and controls can be performed in a suitable governance, risk, and compliance tool with the appropriate functionality and relevant data.

Limitations

QQRRA is based on the concept of excessive residual risk that results from deviations in implementation maturity for a comprehensive set of controls that appropriately specify an organization's risk target. Full implementation of these controls implies an organization's risk target has been met and any remaining risk is acceptable. If controls are improperly specified, e.g., they are assigned based on 'best practices' rather than a valid risk analysis, the control set will more likely than not provide an inadequate definition of the risk target and the results of QQRRA will not be reliable. The importance of a valid risk analysis cannot be stressed enough.

QQRRA as described in this whitepaper is also a 'triage' or 'macro' level analysis in the sense that, while large effects can be identified, smaller effects such as changes to a single control may not be detectable. This is due to the large number of controls that are aggregated based on their control function and then applied to the model. Until the approach is further developed to support this type of analysis, organizations may wish to supplement QQRRA with a more targeted approach such as the one articulated by The Open Group. And, like any risk analysis approach, QQRRA is only as good as the information the analyst is provided.

For example, the assumptions made about the maturity of an 'average' or 'typical' organization in the initial baseline analysis are extremely important to the success of the analysis. When QQRRA is fully integrated into the HITRUST Approach, HITRUST will make every effort to provide reasonable 'optimistic, most likely, and pessimistic' estimates of control maturity based on information obtained from dozens of assessor organizations and thousands of assessments conducted over the past decade and will continue to refine these estimates over time.

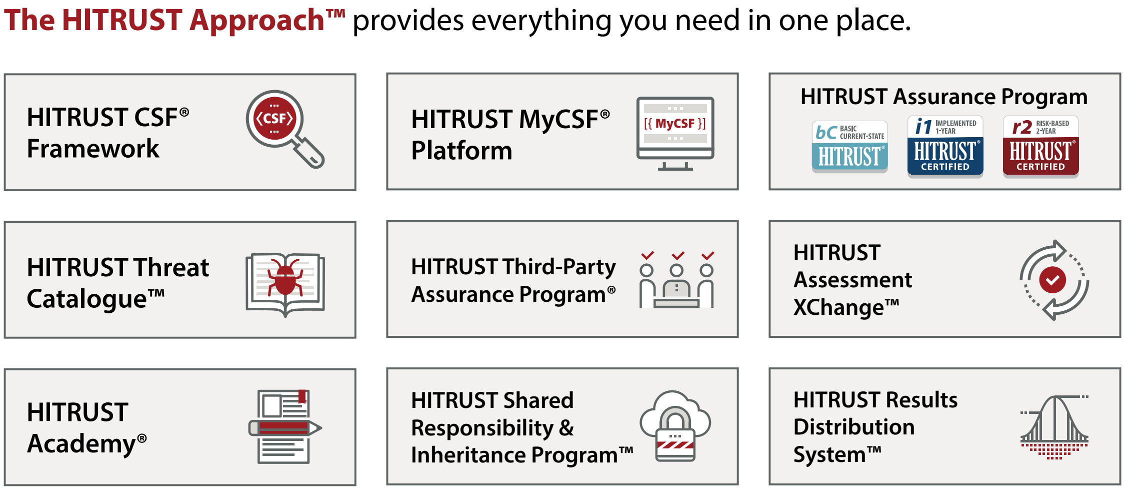
Estimates of excessive residual risk are also based on empirical data that does not distinguish between the acceptable residual risk that exists 'above' the organization's risk target and the unacceptable residual risk that exists 'below' it. Given that risk tolerance(s) can vary significantly from one organization to another, we believe this difference is essentially unknowable for all practical purposes. We subsequently accept that the empirical data obtained about frequencies of occurrence and probable impacts provide reasonable estimates for residual risk analysis. However, we must point out that—while maturity scores close to the organization's risk target will drive the risk estimates to zero—there remains an essentially unknowable amount of residual risk that has been accepted by the organization.

About the Author

Bryan Cline, Ph.D., Chief Research Officer, HITRUST
Bryan provides thought leadership on risk management and compliance and develops the methodologies used in various components of the HITRUST Approach. This includes a focus on the design of the HITRUST CSF and the assessment and certification models used in the HITRUST Assurance Program, for which he provides technical direction and oversight. He is also responsible for addressing emerging trends impacting risk management and compliance to ensure the HITRUST Approach sets the bar for organizations seeking the most comprehensive privacy and security frameworks available. Bryan previously served as HITRUST's Vice President of Standards and Analysis.

About HITRUST

Founded in 2007, HITRUST Alliance is a not-for-profit organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from both the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management and de-identification frameworks; related assessment and assurance methodologies; and initiatives advancing cyber sharing, analysis and resilience, all of which comprise the HITRUST Approach to a comprehensive information security and privacy risk and compliance management ecosystem.



The HITRUST Approach™ provides everything you need in one place.

HITRUST CSF® Framework

HITRUST MyCSF® Platform

HITRUST Assurance Program

HITRUST Threat Catalogue™

HITRUST Third-Party Assurance Program®

HITRUST Assessment XChange™

HITRUST Academy®

HITRUST Shared Responsibility & Inheritance Program™

HITRUST Results Distribution System™

CSF
[{ MyCSF }]
bC BASIC CURRENT-STATE HITRUST
i1 IMPLEMENTED 1-YEAR HITRUST CERTIFIED
r2 RISK-BASED 2-YEAR HITRUST CERTIFIED

Figure 24. The HITRUST Approach

HITRUST also actively participates in many efforts in government advocacy, community building, and cybersecurity education. For more information, visit www.hitrustalliance.net.

Appendix A – Acronyms

AC	Attenuated Capability
ADCM	Average Deterrent Control Maturity
ADeCM	Average Detective Control Maturity
AF	Attenuation Factor
ALE	Annualized Loss Expectancy
AM	Attenuated Motivation
APCM	Average Preventive Control Maturity
ARcCM	Average Recovery Control Maturity
ARO	Annual Rate of Occurrence
ARsCM	Average Responsive Control Maturity
AttRO	Attenuated Rate of Occurrence
AV	Asset Value
C	Capability (Threat Actor)
CEO	Chief Executive Officer
CIPAC	Critical Infrastructure Protection Advisory Council
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CMS	Centers for Medicare and Medicaid Services
CPO	Conditional Probability of Occurrence
CPO(i)	Conditional Probability of Occurrence, Loss Form 'i'
CRO	Chief Research Officer

DAF	Deterrent Attenuation Factor
DeEF	Detective Exposure Factor
DHS	Department of Homeland Security
e	Exponential Function
EF	Exposure Factor
ERM	Enterprise Risk Management
FAIR	Factor Analysis for Information Risk
FC	Fully Compliant
GCC	Government Coordinating Council
H	High
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HPH	Health and Public Health
I	Impact
IP	Internet Protocol
L	Low
L	Likelihood
LR	Lost Revenue
M	Medium or Moderate
M	Motivation (Threat Actor)
MC	Mostly Compliant
ML	Maximum Loss
ML(i)	Maximum Loss, Loss Form "i"

n	Number of periods per annum
N/A	Not Applicable
NC	Non-Compliant
NIST	National Institute of Standards and Technology
NR	Non-operational Risk
NR(i)	Non-operational Risk, Loss Form 'i'
o/a	On or about
OCR	Office of Civil Rights
OR	Operational Risk
ORA	Operational Risk Per Annum
ORP	Operational Risk Per Period
PAF	Preventive Attenuation Factor
PC	Partially Compliant
POA	Probability of Occurrence Per Annum
POP	Probability of Occurrence Per Period
QQRRA	Quasi-Quantitative Residual Risk Analysis
R	Risk; also (total) Risk
RCap	Risk Capacity
RcC	Recovery Costs
RcEF	Recovery Exposure Factor
RcC	Recovery Costs
RO	Rate of Occurrence
ROP	Rate of Occurrence Per Period

RsC	Response Costs
RsEF	Responsive Exposure Factor
SC	Somewhat Compliant
SCC	Sector Coordinating Council
SCRM	Supply Chain Risk Management
SEP	Secondary Event Probability
SEP(i)	Secondary Event Probability, Loss Form ‘i’
SLE	Single Loss Expectancy
SLE(i)	Single Loss Expectancy, Operational Loss Form ‘i’
SRO	Secondary (Event) Rate of Occurrence
SRO(i)	Secondary (Event) Rate of Occurrence, Loss Form ‘i’
TBD	To be Determined
TPRM	Third Party Risk Management
VH	Very High
VL	Very Low

Appendix B – Glossary

Acceptable Risk

The level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific IT system. [NIST Glossary]

Adequate Security [Protection]

Security [protection] commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [NIST Glossary]

Adversary

Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. [NIST Glossary]

Analysis Approach

The approach used to define the orientation or starting point of the risk assessment, the level of detail in the assessment, and how risks due to similar threat scenarios are treated. [NIST Glossary]

Assessment

See Security Control Assessment or Risk Assessment.

Assessment Scope

The information systems and technology, infrastructure, and organizational elements that are the target of assessment. [HITRUST]

Asset(s)

Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards). [NIST Glossary]

Assurance

Grounds for justified confidence that a claim has been or will be achieved.

Note 1: Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated.

Note 2: Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims. [NIST Glossary]

Attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [NIST Glossary]

Attack Surface

The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment. [NIST Glossary]

Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NIST Glossary]

Availability

Ensuring timely and reliable access to and use of information. [NIST Glossary]

Avoidance Control

A general class of control that helps minimize a target's attack surface or otherwise reduce the frequency with which a threat actor comes into contact with an asset. [HITRUST]

Capability (Threat Actor)

The ability of a threat actor to successfully exploit one or more vulnerabilities to achieve an objective and generally consists of a threat actor's knowledge, skills, and tools (and other resources). [HITRUST]

Care

The process of protecting someone or something and providing what that person or thing needs. [Cambridge Dictionary]

Compensating Security Control(s)

A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system. [NIST Glossary]

Compliance

An adherence to the laws, regulations, standards, guidelines, and other specifications [such as contractual obligations] relevant to an organization's business. [Adapted from the HITRUST Risk vs. Compliance Whitepaper, p. 3]

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [NIST Glossary]

Control Category(ies)

The highest topical level in the HITRUST CSF control framework. [HITRUST]

Control Function

The manner in which a control addresses a threat to manage associated risk. [HITRUST]

Control Implementation Requirement

A granular, often prescriptive requirement or activity within a HITRUST CSF control intended to help an organization achieve the outcome indicated by its Control Specification. [HITRUST]

Control Maturity

The extent to which a control is defined, implemented, measured, managed/controlled, and effective. [HITRUST] Also, 'Control Implementation Maturity.'

Control Purpose

Synonymous with Control Function.

Control Requirement

See Control Implementation Requirement.

Control(s)

The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature. An attribute assigned to an asset that reflects its relative importance or necessity in achieving or contributing to the achievement of stated goals. [NIST Glossary] Synonymous with 'Countermeasures' and 'Safeguards.'

A [HITRUST CSF] control is a collection of implementation requirements intended to satisfy the objective or outcome [identified] by a control specification; includes a control reference, i.e., a control number and name, risk factors, topical area tags, and supporting authoritative sources. [HITRUST]

Corrective Action

Activities intended to remediate control deficiencies; actions taken to address causes of non-conformity, preclude hazards, or prevent the recurrence of a problem. [HITRUST]

Corrective Action Plan (CAP)

Corrective actions for an issuer for removing or reducing deficiencies or risks identified by the Assessor during the assessment of issuer operations. The plan identifies actions that need to be performed in order to obtain or sustain authorization. [NIST Glossary]

Countermeasure(s)

Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. [NIST Glossary] Synonymous with 'Controls' or 'Safeguards.'

Criticality

A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. Note criticality is often determined by the impact to the organization due to a loss of integrity or availability. [NIST Glossary]

Cyber Attack

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. [NIST Glossary]

Cyber Incident

Actions through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See Incident. [NIST Glossary]

Cyber Risk

Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system. [NIST Glossary]

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation. [NIST Glossary]

Cyberspace

The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. [NIST Glossary]

Data

Information in a specific representation, usually as a sequence of symbols that have meaning [or] pieces of information from which 'understandable information' is derived. [NIST Glossary]

Decision Analysis

Logical methods for improving decision-making … [including] models for decision-making under conditions of uncertainty or multiple objectives; techniques of risk analysis and risk assessment; experimental and descriptive studies of decision-making behavior; economic analysis of competitive and strategic decisions; techniques for facilitating decision-making by groups; and computer modeling software and expert systems for decision support. [Decision Analysis Society]

Decision Support Control

A general class of control that involves actions taken to facilitate the decision analysis process and improve decision-making. [HITRUST]

Detective Control

A general class of control that involves the monitoring and identification of potential threat events. [HITRUST]

Deterrent Control

A general class of control that helps discourage a threat actor from initiating or taking advantage of (exploit) a contact. [HITRUST]

Diligence

[The] earnest and persistent application of effort, especially as required by law. [FindLaw Dictionary]

Due Care

The care that an ordinarily reasonable and prudent person would use under the same or similar circumstances; also called ‘ordinary care’ or ‘reasonable care.’ [FindLaw Dictionary]

The level of care expected from a reasonable person of similar competency under similar conditions. [ISACA Glossary]

Due Diligence

Such diligence as a reasonable person under the same circumstances would use; use of reasonable but not necessarily exhaustive efforts; also called ‘reasonable diligence.’ [FindLaw Dictionary]

The performance of those actions that are generally regarded as prudent, responsible, and necessary to conduct a thorough and objective investigation, review, and/or analysis. [ISACA Glossary]

Enhanced Overlay

An overlay that adds controls, enhancements, or additional guidance to security control baselines in order to highlight or address needs specific to the purpose of the overlay. See Overlay. Synonymous with Tailored Overlay. [NIST Glossary]

Event

Any observable occurrence in an information system. [NIST Glossary]

Factor Analysis of Information Risk (FAIR)

An international standard quantitative model for understanding, analyzing, and quantifying cyber risk and operational risk in financial terms. [FAIR]

Impact

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [NIST Glossary]

Impact Level

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [NIST Glossary] Synonymous with Impact Value.

Impact Value

The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high. [NIST Glossary] Synonymous with Impact Level.

Incident

An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [NIST Glossary]

Information

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. [NIST Glossary] Not to be confused with the term 'Data.'

Information Security Risk

The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. See Risk. [NIST Glossary]

Information System-Related Security Risk

Risk that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, other organizations, and the Nation. A subset of Information Security Risk. See Risk. [NIST Glossary]

Inherent Risk

Risk that exists when the status of key controls is not taken into consideration or is otherwise unknown. [HITRUST]

Integrity

Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [NIST Glossary]

Likelihood

A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. [NIST Glossary]

Likelihood of Occurrence

See Likelihood.

Maturity Model

A set of characteristics, attributes, or indicators that represent progression in a particular domain. A maturity model allows an organization or industry to have its practices, processes, and methods evaluated against a clear set of requirements (such as activities or processes) that define specific maturity levels. At any given maturity level, an organization is expected to exhibit the capabilities of that level.

A tool that helps assess the current effectiveness of an organization and supports determining what capabilities they need in order to obtain the next level of maturity in order to continue progression up the levels of the model. [CERT RMM v1.2]

Measure(s)

The results of data collection, analysis, and reporting. [NIST Glossary]

A standard used to evaluate and communicate performance against expected results (measures are normally quantitative in nature capturing numbers, dollars, percentages, etc., but can also address qualitative information such as customer satisfaction; reporting and monitoring measures help an organization gauge progress toward effective implementation of strategy). [ISACA Glossary]

Measurement

The process of data collection, analysis, and reporting. [NIST Glossary]

Measurements are "observations that quantitatively reduce uncertainty." [Hubbard, D., Seiersen, R., Geer Jr., D., and McClure, S. (2016)]

Metric(s)

Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. [NIST Glossary]

A quantifiable entity that allows the measurement of the achievement of a process goal (metrics should be SMART—specific, measurable, actionable, relevant, and timely; complete metric guidance defines the unit used, measurement frequency, ideal target value (if appropriate), and also the procedure to carry out the measurement and the procedure for the interpretation of the assessment). [ISACA Glossary]

Motivation (Threat Actor)

The drivers—be it emotional or the pursuit of supremacy or material gain—that causes a threat actor to commit harmful acts. [Derived from Intel]

Ontology

In the context of computer and information sciences, an ontology defines a set of representational primitives with which to model a domain of knowledge or discourse. The representational primitives are typically classes (or sets), attributes (or properties), and relationships (or relations among class members). The definitions of the representational primitives include information about their meaning and constraints on their logically consistent application. [Gruber]

Operational Risk

Risk of loss resulting from inadequate or failed internal process, people, and systems or from external events. Includes legal risk, but excludes strategic and reputational risk [Basel Committee]

Overlay

A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process that is intended to complement (and further refine) security control baselines [to fit the user's specific environment and mission]. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. [NIST Glossary]

Plan of Action and Milestones

A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. Synonymous with Corrective Action Plan. [NIST Glossary]

Policy

Overall intention and direction as formally expressed by management, most often articulated in documents that record high-level principles or course of actions; the intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives, and strategic plans established by the enterprise's management teams. [Adapted from the ISACA Glossary]

Possible

Able to be done or achieved, or able to exit. [Cambridge Dictionary]

Preventive Control

A general class of controls that help reduce the likelihood a threat event will occur (or decrease their frequency of occurrence). [HITRUST]

Probable

Likely to be true or likely to happen. [Cambridge Dictionary]

Procedure

A detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes. [Adapted from the ISACA Glossary]

Qualitative Assessment

A set of methods, principles, or rules for assessing risk based on non-numerical categories or levels. [NIST Glossary]

Quantitative Assessment

A set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment. [NIST Glossary]

Quasi-quantitative Assessment

See Semi-quantitative Assessment.

Recovery Control

A general class of control that involves actions taken to restore an organization to a pre-threat event state. [HITRUST]

Rely-ability

The ability of a stakeholder to rely upon the assurances provided by an entity. (HITRUST)

Rely-able Assurances that provide a high degree of rely-ability. [HITRUST]

Repeatablilty The ability to repeat an assessment in the future, in a manner that is consistent with, and hence comparable to, prior assessments. [NIST Glossary]

Reproducibility The ability of different experts to produce the same results from the same data. [NIST Glossary]

Residual Risk Portion of risk remaining after security measures have been applied. [NIST Glossary]

Responsive Control A general class of control that involves actions taken to mitigate the potential impact of a threat event. [HITRUST]

Risk The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [NIST Glossary]

Risk Acceptance The formal acceptance of a specific amount of risk by an individual or organization. [HITRUST]

Risk Analysis The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. [NIST Glossary]

Risk Appetite The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value. [NIST Glossary]

Risk Assessment The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations, resulting from the operation of an information system. Part of risk management, risk assessment incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. [NIST Glossary]

Risk Assessment Methodology A risk assessment process, together with a risk model, assessment approach, and analysis approach. [NIST Glossary]

Risk Avoidance The elimination of risk by not engaging in a specific activity. [HITRUST]

Risk Capacity The maximum amount of risk that an organization can absorb without disrupting achievement of its objectives. [HITRUST]

Risk Evaluation

The process of comparing the estimated risk against given risk criteria to determine the significance of the risk. [ISACA Glossary]

Risk Factor

A characteristic in a risk model as an input to determining the level of risk in a risk assessment. [NIST Glossary]

Risk Management

The total process of identifying, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. [NIST Glossary]

Risk Management Framework

A structured approach used to oversee and manage risk. [NIST Glossary]

Risk Mitigation

Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. [A subset of Risk Response.] [NIST Glossary]

Risk Model

A key component of a risk assessment methodology—in addition to the assessment approach and analysis approach—that defines key terms and assessable risk factors. [NIST Glossary]

Risk Monitoring

Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions. [NIST Glossary]

Risk Response

Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, or other organizations. See Course of Action. Synonymous with Risk Treatment. [NIST Glossary]

Risk Target

The desired level of risk that optimizes an organization's business objectives. [HITRUST]

Risk Tolerance

The level of risk an entity is willing to assume in order to achieve a potential desired result for a specific activity. [NIST Glossary, adapted]

Risk Transference

The redirecting or sharing of risk with another party, e.g., through insurance or indemnification. [HITRUST]

Risk Treatment

Selecting and implementing mechanisms to modify risk. Risk treatment options can include avoiding, optimizing, transferring, or retaining [accepting] risk. [ENISA]

Safeguard(s)

Protective measures prescribed to meet the privacy (e.g., data quality, transparency of use of personal data) and security (e.g., confidentiality, integrity, and availability) requirements specified for an information system. Safeguards may include privacy and security features, management constraints, personal data minimization, use limitations for personal data, personnel security, and security of physical structures, areas, and devices. Synonymous with 'Security Controls' and 'Countermeasures.' [NIST Glossary, adapted]

Scoping

The act of applying scoping guidance, which consists of specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security and privacy controls in the control baseline. [NIST Glossary, adapted from Scoping Guidance]

Scoping Considerations

A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of security controls in the security control baseline. Areas of consideration include policy/regulatory, technology, physical infrastructure, system component allocation, operational/environmental, public access, scalability, common control, and security objective. [NIST Glossary]

Security Assessment

See Security Control Assessment.

Security Control Baseline

A set of information security controls that has been established through information security strategic planning activities intended to be the initial security control set selected for a specific organization and/or system(s) that provides a starting point for the tailoring process. [NIST Glossary]

Security Control(s)

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an organization and/or information system(s) to protect information confidentiality, integrity, and availability. [NIST Glossary, adapted]

Security Control(s) Assessment

The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. [NIST Glossary]

Semi-quantitative Assessment

Use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. Synonymous with Quasi-Quantitative Assessment. [NIST Glossary]

Sensitivity

A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. [NIST Glossary]

Service

An act or activity performed on behalf of another party. [HITRUST]

Standard of Care

The degree of care or competence that one is expected to exercise in a particular circumstance or role. [FindLaw Dictionary]

Tailored Overlay

See Enhanced Overlay.

Tailored Security Control Baseline

A set of security controls resulting from the application of tailoring guidance to the security control baseline. See Tailoring. [NIST Glossary]

Tailoring The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements. [NIST Glossary]

Taxonomy A system for classifying multifaceted, complex phenomena according to common conceptual domains and dimensions. [Bradley]

Threat Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [NIST Glossary, adapted]

Threat Actor An individual or group posing a threat. [NIST Glossary]

Threat Assessment/Analysis Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. [NIST Glossary]

Threat Event An event or situation that has the potential for causing undesirable consequences or impact. [NIST Glossary]

Frequency (f) The rate of a repetitive event. If T is the period of a repetitive event, then the frequency f is its reciprocal, 1/T. Conversely, the period is the reciprocal of the frequency, T = 1 / f. (NIST Glossary]

Threat Scenario A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time. [NIST Glossary]

Threat Source The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability. [NIST Glossary].

Total Risk The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). [NIST Glossary]

Variance The state of being variable, different, divergent, or deviate; a degree of deviation. [English Encyclopedia]

Variance Reduction Control A general class of control that involves actions taken to reduce the variability in the output of a process without affecting its intended purpose. [HITRUST]

Variation A change in data, characteristic or function caused by one of four factors: special causes, common causes, tampering, or structural variation. [ASQ Glossary]

Vulnerability Assessment/ Analysis Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [NIST Glossary]

Vulnerability Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [NIST Glossary]

Weakness A particular part or quality of someone or something that is not good or effective (e.g., an error or defect). [Cambridge Dictionary, adapted]

Appendix C – References

ASQ (2022a). Quality Resources: Six Sigma. Available from https://asq.org/quality-resources/six-sigma.

ASQ (2022b). Quality Glossary. Available from https://asq.org/quality-resources/quality-glossary/.

Banking and Financial Services BA (2012, May 10). Basil II – Direct vs. Indirect Operational Loss (Blog). Available from https://bfsba.wordpress.com/2012/05/10/basel-ii-direct-vs-indirect-loss/.

Basel Committee on Banking Supervision (2011, Jun). Principles for the Sound Management of Operational Risk. Basel, CH: Author. Available from https://www.bis.org/publ/bcbs195.pdf.

Blum, D. (2020). Rational Cybersecurity for Business: The Security Leader's Guide to Business Alignment. Apress: Silver Springs, MD. Available from https://learning.oreilly.com/library/view/rational-cybersecurity-for/9781484259528/htmel/Cover.xhtml.

Bowen, P. and Kissel, R. (2007, Jan). Program Review for Information Security Management Assistance (PRISMA) [NISTIR 7358]. Gaithersburg, MD: NIST. Available from https://csrc.nist.gov/publications/detail/nistir/7358/final.

Bradley, E. H., Curry, L. A., and Devers, K. J. (2007). Qualitative data analysis for health services research: developing taxonomy, themes, and theory. Health services research, 42(4), 1758–1772. Available from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1955280/pdf/hesr0042-1758.pdf.

Cambridge (2022). Dictionary. Available from https://dictionary.cambridge.org/dictionary/.

CBRN Centres of Excellence (2015, Dec). How to Implement Security Controls for an Information Security Program at CBRN Facilities, p. 1. Available from https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-25112.pdf.

Centers for Medicare and Medicaid Services, CMS (2017). CMS Acceptable Risk Safeguards (ARS) (CMS_CIO-STD-SEC01-3.0). Baltimore, MD: Author. Available from https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-30-Publication.html.

CISA (2022a). Critical Infrastructure Partnership Advisory Council. Available from https://www.cisa.gov/critical-infrastructure-partnership-advisory-council.

CISA (2022b). Infrastructure Security: Critical Infrastructure Sector Partnerships: Sector Coordinating Councils. Available from https://www.cisa.gov/sector-coordinating-councils.

Cline, B. (2017, Sep). Leveraging a Control-Based Framework to Simplify the Risk Analysis Process, ISSA Journal, 15(9), pp. 39-42. Available from https://hitrustalliance.net/content/uploads/2016/01/Leveraging-a-Control-Based-Framework-to-Simplify-the-Risk-Analysis-Process.pdf.

Cline, B. (2018, Feb). Risk Analysis Guide for HITRUST Organizations & Assessors: A guide for self and third-party assessors on the application of HITRUST's approach to risk analysis. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf.

Cline, B., Huval, J., and Sheth, B. (2019, Oct). Evaluating Control Maturity Using the HITRUST Approach: Quasi-quantitative scoring based on the HITRUST CSF security and privacy control implementation maturity model. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.

CMS (2015). Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E Document Suite, Version 2.0). Baltimore, MD: Author. Available from https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf.

Department of the Navy (2008, Jul 15). DoD Information Assurance Certification and Accreditation Process (DIACAP) Handbook, Version 1.0. Washington, D.C.: Author.

Forrester (2019, Aug). The Real Costs of Planned and Unplanned Downtime: Accelerate Recovery with New Technologies (Report). Available from https://www.ibm.com/downloads/cas/L57KW7ND.

Freund, J. and Jones, J. (2015). Measuring and Managing Information Risk: A FAIR Approach. New York: Elsevier.

Gruber, T. (2009). Ontology. In L. Liu and M. Tamer Ozsu (Eds.) Encyclopedia of Database Systems, L. Liu and M. Tamer Ozsu (Eds.). Springer-Verlag. Available from https://tomgruber.org/writing/definition-of-ontology.pdf.

Hansche, S., Berti, J., and Hare, C. (2004). Official (ISC)2 Guide to the CISSP Exam. Boca Raton, FL: Auerbach.

Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, U.S. Statutes at Large 110 (1996): 1936-2103. https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

HHS (2022a). HIPAA: HIPAA Home: For Professionals: Covered Entities and Business Associates. Available from https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

HHS (2022b). HIPAA: HIPAA Home: HIPAA for Professionals. Available from https://www.hhs.gov/hipaa/for-professionals/index.html.

HHS (2022c). HHS: HIPAA Home: For Professionals: The Security Rule. Available from https://www.hhs.gov/hipaa/for-professionals/security/index.html.

HHS (2022d). Home: About HHS. Available from https://www.hhs.gov/about/index.html.

HHS (2022e). HHS: OCR Home: About Us. Available from https://www.hhs.gov/ocr/about-us/index.html.

HHS (2022f). HHS: HIPAA Home: For Professionals: HIPAA Compliance and Enforcement: Resolution Agreements. Available from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.

Highmark (2022). Your Health Care Partner. Available from https://www.highmark.com/hmk2/index.shtml.

HITRUST (2021). HITRUST Threat Catalogue. Frisco, TX: Author. Available by registering and accepting the license agreement at https://hitrustalliance.net/hitrust-threat-catalogue-registration/.

HITRUST (2022a). The HITRUST Approach. Available from https://hitrustalliance.net/the-hitrust-approach/.

HITRUST (2022b). HITRUST CSF. Available from https://hitrustalliance.net/hitrust-csf/.

HITRUST (2022c). Assurance Program. Available from https://hitrustalliance.net/hitrust-assurance-program/.

HITRUST (2022d). HITRUST Threat Catalogue. Available from https://hitrustalliance.net/threat-catalogue/.

Hubbard, D., Seiersen, R., Geer Jr., D., and McClure, S. (2016). How to Measure Anything in Cybersecurity Risk. Hoboken, NJ: John Wiley & Sons.

Informs (2022). Decision Analysis Society: About Us. Available from https://connect.informs.org/das/home.

Joint HPH Cybersecurity WG (2016, May). Healthcare Sector Cybersecurity Framework Implementation Guide. Available from https://hitrustalliance.net/uploads/HPHCyberImplementationGuide.pdf.

JTF (2020, Oct). Control Baselines for Information Systems and Organizations (NIST SP 800-53B). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.

JTF TI (2011, Mar). Managing Information Security Risk: Organization, Mission, and Information System View (NIST SP 800-39). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

JTF TI (2012, Sep). Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Kissel, R. (Ed.) (2013). Glossary of Key Information Security Terms (NISTIR 7298, Revision 2). Gaithersburg, MD: NIST. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

Kreitner, R. (1995). Management (6th ed.). New York: Houghton Mifflin College Division, p. 4.

Lartey, P., Kong, Y., Bah, F., Santosh, R., and Gumah, I. (2019, Aug). Determinants of Internal Control Compliance in Public Organizations; Using Preventive, Detective, Corrective and Directive Controls. In International Journal of Public Administration, p. 4. Available from https://www.researchgate.net/profile/Isaac-Akolgo/publication/335082288_Determinants_of_Internal_Control_Compliance_in_Public_Organizations_Using_Preventive_Detective_Corrective_and_Directive_Controls/links/5d86d58e458515cbd1af4117/Determinants-of-Internal-Control-Compliance-in-Public-Organizations-Using-Preventive-Detective-Corrective-and-Directive-Controls.pdf

Law Insider (2022). Dictionary: Business Process. Available from https://www.lawinsider.com/dictionary/business-process.

Merriam-Webster (2022). Homepage. Available from https://www.merriam-webster.com/.

Miller, L. and Gregory, P. (2012). CISSP for Dummies (4th ed.). New York: Wiley.

NIST (2004). Standards for Security Categorization of Federal Information and Information Systems (FIPS Pub 199). Gaithersburg, MD: Author. Available from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

NIST (2018, 16 Apr). Framework for Improving Critical Infrastructure Cybersecurity (v1.1). Gaithersburg, MD: Author. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

NIST (2020). Information Technology Laboratory Computer Security Resources: Glossary. Available from https://csrc.nist.gov/glossary.

NIST (2022a). About NIST. Available from https://www.nist.gov/about-nist.

NIST (2022b). Information Technology Laboratory: Computer Security Resource Center: Glossary. Available from https://csrc.nist.gov/glossary.

NIST (2022c). National Online Informative References Program: Informative Reference Catalog. Available from https://csrc.nist.gov/projects/olir/informative-reference-catalog?infRef=10041&sortBy=2.

PHE (2022). Preparedness: Planning: Critical Infrastructure Protection: Healthcare and Public Health (HPH) Sector. Available from https://www.phe.gov/Preparedness/planning/cip/HPH/Pages/default.aspx.

Richards, D., Oliphant, A., and Le Grand, C. (2005, Mar). Global Technology Audit Guide: Information Technology Controls (GTAG 1). Altamonte Springs, FL: The Institute of Internal Auditors. Available from https://pdf4pro.com/cdn/gtag-1-information-technology-controls-26aa03.pdf.

Riskope (2017, Feb 1). Making Sense of Probabilities and Frequencies. Available from https://www.riskope.com/2017/02/01/making-sense-probabilities-frequencies/.

Rossebo, J., Fransen, F., and Luiijf, E. (2016, Apr). Including threat actor capability and motivation in risk assessment for Smart Grids. IEEE Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG). See workshop presentation available from https://project-sparks.eu/wp-content/uploads/2016/04/rossebo-cpsr-sg-paper-one.pdf.

Sophos (2021, Apr). The State of Ransomware 2021. Available from https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf.

Stine, K., Quinn, S., Witte, G., and Gardner, R. (2020, Oct). Integrating Cybersecurity and Enterprise Risk Management (ERM) (NISTIR 8286). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf.

Van Fleet, D. and Seperich, G. (2013). Agribusiness: Principles of Management (International ed.) New York: CENGAGE, p. 24.

Wasson, J. and Bluesteen, C. (2017, Apr). Cognitive Defense: Influencing the Target Choices of Less Sophisticated Threat Actors. In Homeland Security Affairs (13). Available from https://www.hsaj.org/resources/uploads/2022/04/Cognitive-Defense-1.pdf.

Williams, C., Donaldson, S., and Siegal, S. (2020). Building an Effective Security Program. Boston: De Gruter.

HITRUST®

FOR MORE INFORMATION:

Contact your HITRUST Product Specialist
Call: 855-448-7878 or Email: sales@hitrustalliance.net

www.hitrustalliance.net