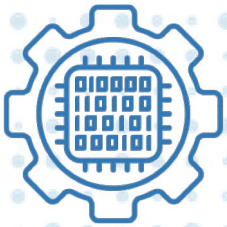


Cyber-Informed Engineering

Cyber-Informed Engineering (CIE) Benefits Quantification

Recommendations for Consideration

September 30, 2024

Authors:

Daniel Rebori-Carretero
MITRE

Lauren Graham
MITRE

Nate Adams
MITRE

Sarah Freeman
MITRE

INL/MIS-24-81663-Rev000

Cyber-Informed Engineering (CIE) Program activities are sponsored by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER) and performed by Idaho National Laboratory and the National Renewable Energy Laboratory.

The authors of this report acknowledge and appreciate the sponsorship of the CIE Program partners and the contributions from the CIE Community of Practice (COP) members.

Contents

1. Background 4
2. Security Challenges and Difficulty Measuring CIE Value 4
3. Potential Approaches for CIE Benefits Quantification 9
3.1. Option #1: Calculating the Value of a Specific CIE Implementation 9
3.2. Option #2: Consequence or Impact Reduction Following a Cyber-Attack 10
3.3. Option #3: Reducing Security Costs through Proactive Investment 12
3.4. Option #4: Addressing Organizational Susceptibility to Cyber-Attacks 14
3.5. Option #5: Measuring "Future-Proofing" Critical Infrastructure 15
4. Recommended Path Forward 28
5. Acronyms 29
Appendix A: Evaluated Analytic Methodologies 30
A.1 Factor Analysis of Information Risk (FAIR) 31
A.2 Value Analysis or Value Engineering (VAVE) 34
A.3 Cyber Value-at-Risk (CVaR) 35
A.4 Process Hazard Analysis (PHA) / Cyber PHA 37
A.5 Layers of Protection Analysis (LOPA) 38
A.6 Infrastructure Susceptibility Analysis (ISA) 40

1. Background

Cyber-Informed Engineering (CIE) integrates engineering considerations into the conception, design, development, and operation of any cyber-physical system (CPS), mitigating (or eliminating) impacts of cyber-enabled attacks. In July 2024, Idaho National Laboratory (INL) tasked MITRE researchers to investigate methods to systematically measure the value from implementation of CIE. Additionally, INL tasked MITRE to consider methods to:

- Measure CIE implementation success elements and outcomes;
- Identify (and calculate) the value from early adoption of CIE; and,
- Determine (and calculate) the business justification for CIE implementation, especially on existing infrastructure.

To support this activity, MITRE researchers reviewed existing approaches within the engineering and cybersecurity domains to understand how organizations identify, evaluate, and prioritize security investments. The strengths and weaknesses of each of these methods were considered, as well as the applicability and use to CIE stakeholders. Based on this research, MITRE proposed potential approaches for CIE benefits quantification, as well as a recommendation for INL consideration and concurrence.

2. Security Challenges and Difficulty Measuring CIE Value

Throughout the course of this analysis, MITRE researchers determined several challenges within the field of industrial security that may inhibit future CIE benefits calculations. Overcoming some of these challenges may require acceptance of starting assumptions to properly focus CIE success metrics:

Lack of Common Language or Security Taxonomy

Throughout their review, MITRE researchers observed that organizations lack a common language to describe the security concepts (e.g., resiliency, value, vulnerability, susceptibility, etc.). Some researchers and professionals have proposed that without this common taxonomy, security requirements are inconsistently levied across sectors and industries.[1] Considering the process of defining CIE implementation "success," the lack of a common language may challenge attempts to quantify CIE value. Currently, MITRE is not proposing the creation of a complete security taxonomy; however, we acknowledge the need to clearly define CIE value propositions and the metrics within the CIE benefits quantification methodology. (Potentially relevant terms and concepts are included below; this list is not all inclusive.)

[1] Firesmith, Donald. "A Taxonomy of Security-Related Requirements." Carnegie Mellon University, 2005. https://insights.sei.cmu.edu/documents/235/2005_019_001_30112.pdf.

Critical Terms within Security Dialogues			
Benefit	Capability	Consequence	Cost
Intent	Resilience	Resiliency	Risk
Safety	Security Maturity	Susceptibility	Threat
Value	Vulnerability	Impact	

Competing Priorities and Limited Resources in Operations

All organizations, including critical infrastructure asset owners/operators, must balance competing operational and security priorities within their enterprise. In 2023, defenders faced 26,447 vulnerabilities, nearly 1,500 more than disclosed the previous year.[2] Additionally, typical operations face other, non-security related requirements, such as investments in capital or other improvements that may not be security related. In this environment, organizational leadership must determine how to effectively distribute and employ limited resources such as time, money, and personnel.

For security professionals (and the CIE team), security improvements and mitigations must be measured against other investments that could be made by the organization. In this environment, properly articulating return-on-investment (ROI), or anticipated ROIs, becomes even more critical, as is the ability for security leadership to quantify the potential risk to the organization as it shifts over time. Because of this need, MITRE assessed that any CIE benefits qualification approach must be able to be applied proactively (in addition to retrospectively) in order to support the business function of prioritizing investments.

Insufficient Cyber Event Data Inhibits Effectiveness of Quantitative Analysis

As mentioned previously, despite an ever-increasing list of cyber-attacks, detailed analysis of losses following an event are often not available outside the victim organization. It has been assessed that the rise of cyber insurance would make this information more readily available; however, much of it remains unavailable to the common security professional (beyond meta-analyses such as CISA's 2020 analysis).[3] This lack of data (or at least lack of access to high-quality, high-fidelity data) may prove detrimental to CIE programmatic efforts designed to calculate the value of CIE implementation, particularly at the macro level. This may require that the CIE benefits quantification methodology adopt several starting assumptions (e.g., the average cost of a cybersecurity breach is *x*) to calculate potential CIE gains.

---

[2] Abbasi, Saeed. "2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is | Qualys Security Blog." Qualys, December 19, 2023. https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one.

[3] "Cost of a Cyber Incident: Systematic Reivew and Cross-Validation." Cybersecurity & Infrastructure Security Agency (CISA), October 26, 2020. https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf.

Challenges in Identifying 'Control' Organization Limits Comparative Analysis

One method for addressing a dearth of incident data is to leverage comparative values, rather than averages. In this case, benefits calculations consider two "paths": one with CIE principal adoption and one without. This enables a comparison against an experimental control (i.e., the organization that forgoes CIE) and CIE adoptees, in which the CIE gains are articulated as the difference between the two organizations (e.g., *Organization A (with CIE) has experienced fewer disruptive cyber events over the last five years as compared to Organization B; Organization A spends 50 percent less on their operational security budget as compared with Organization B, etc.*). However, identifying suitable candidate organizations (and gaining access to necessary data) for this type of analysis can be challenging, particularly given the desire to compare two organizations of similar size and resources with similar industry/sector constraints.

Alternatively, the comparative analysis can be conducted against the same organization but at different times (i.e., the time before CIE (i.e., *Before CIE*) and the time after (i.e., *Anno CIE*)), where CIE adoption has resulted in some positive outcomes (e.g., reduced plant outages, reduced operational security costs, etc.). In this case, the difficulty is shifted towards identifying a willing partner to make the argument of CIE adoption through individual 'use cases.'

Implementation of CIE Benefits Extend Beyond Traditional Metrics

In the late 1990s and early 2000s, the economics of security (at least as it related to information technology (IT) applications) rose in prominence, with a body of literature promoting the benefits of economic analysis to justify security investments.[4] Although numerous variations exist, three measurements or metrics comprise the foundation of economic analysis within the IT domain:

1. **Loss** defined as loss following an event, or the value at risk were an intrusion, breach, or failure to occur;
2. **Vulnerability**, which is often defined as a probability that captures the chances of realizing some or all the loss; and,
3. **Effectiveness** defined as the effectiveness of a given solution or mitigation.[5]

Limiting CIE value to metrics within these three domains, however, results in an incomplete picture of the CIE adoption benefits. For example, the CIE Principle "Organizational Culture" addresses added dimensions beyond reduced losses following an intrusion, breach, or failure. Instead, measurement of the potential or realized benefits of this principle include those of extrinsic value or qualitative in nature. Described another way, CIE Principles promote benefits (see Table 1) that are the direct result of adoption (i.e., primary benefits), as well as secondary benefits (i.e., ancillary or indirect). Ideally, any benefits quantification methodology adopted by the CIE program would be able to measure the full value of CIE implementation including both primary and secondary benefits.

---

[4] Wilson, Bradley, Mark Arena, Lauren Mayer, Chad Heitzenrater, Jason Mastbaum, and Kevin Connolly. "A Methodology for Quantifying the Value of Cybersecurity Investments in the Navy." RAND, n.d.

[5] Wilson, Bradley, Mark Arena, Lauren Mayer, Chad Heitzenrater, Jason Mastbaum, and Kevin Connolly. "A Methodology for Quantifying the Value of Cybersecurity Investments in the Navy." RAND, n.d.

Table 1: Selective List of CIE Adoption Benefits.

	PRINCIPLE	KEY QUESTION	PRIMARY BENEFITS	SECONDARY BENEFITS
1	**Consequence-Focused Design**	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?	Improved system protection and resilience against worst possible attacks and consequences	Improved protection and resilience against unforeseen and future attacks
2	**Engineered Controls**	How do I select and implement controls to reduce avenues for attack or the damage that could result?	Engineered controls reduce the impact from potential adverse cyber-events	Engineered controls are more effective than traditional security controls and are less likely to introduce "friction" into business/engineering operations
3	**Secure Information Architecture**	How do I prevent undesired manipulation of important data?	Reduced instances of data loss or corrupted data	Identification (and mitigation) of single points of failure introduced through data source interdependencies
4	**Design Simplification**	How do I determine what features of my system are not absolutely necessary to achieve the critical functions?	Simplified design reduces the attack surface available to the adversary	Simplified design results in fewer system outages from "hidden weaknesses" or sources of unverified trust
5	**Layered Defenses**	How do I create the best compilation of system defenses?	Increased number and diversity of defenses, which decrease the chance of adversarial success and cyber-attack impact	Reduced reliance on a single defensive solution (or vendor), which provides additional operational flexibility to the organization to address or mitigate identified security concerns
6	**Active Defense**	How do I proactively prepare to defend my system from any threat?	Increased number of deployed proactive security solutions	Increased variety of defenses challenges adversary operations
7	**Interdependency Evaluation**	How do I understand where my system can impact others or be impacted by others?	Reduced downtime due to sources of "unverified trust"	Increased contingency planning within the organization results in increased resiliency

	PRINCIPLE	KEY QUESTION	PRIMARY BENEFITS	SECONDARY BENEFITS
8	**Digital Asset Awareness**	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?	Reduced time required for emergency mitigation or patch management	Increased organizational awareness; deliberate (versus unintentional) deployment of digital asset features and functionality
9	**Cyber-Secure Supply Chain Controls**	How do I ensure my providers deliver the security the system needs?	Increased supplier compliance with required security controls	Proactively identifying and implementing a more robust security posture reduces ongoing operational security costs (particularly those resulting from an acute security incident)
10	**Planned Resilience**	How do I turn “what ifs” into “even ifs”?	Reduced recovery time following an event	Security teams are more likely to focus on strategic security investments (rather than tactical response)
11	**Engineering Information Control**	How do I manage knowledge about my system? How do I keep it out of the wrong hands?	Increased number of information controls	Proactive identification of critical information sources that may otherwise be overlooked
12	**Organizational Culture**	How do I ensure that everyone’s behavior and decisions align with our security goals?	Increased adoption of proactive (rather than reactive) security	Increased communication throughout the organization regarding potential adverse events, as well as past events, which better prepares less experienced staff

3. Potential Approaches for CIE Benefits Quantification

Based on a review of previous approaches to prioritize cybersecurity investments or to calculate ROIs of past investments, MITRE researchers identified five potential methods to calculate CIE value.

3.1. Option #1: Calculating the Value of a Specific CIE Implementation

Hypothesis

Implementation of CIE-inspired controls provide great returns of investment as compared to non-CIE developed controls.

A review of the body of literature around cybersecurity investments identifies several similar approaches intended to calculate the "return on investment" for a specific cybersecurity deployment.[6,7] In general, these approaches can be summarized as the difference between the benefit of a given solution and its cost effectiveness of a given solution and is typically rendered as a percentage. (It should be noted, that in this design, those investments with the greatest (positive) difference between the benefit and cost is preferred (i.e., benefit > cost)):

$$ROI = \left(\frac{benefit - cost}{cost}\right)$$

$Where,$
$Benefit = reduction\ in\ risk\ or\ other\ value\ of\ a\ given\ solution$
$Cost = the\ cost\ to\ implement\ a\ given\ security\ solution$

Considering this option, the ROI calculation can be used to calculate the return of a specific CIE-derived solution or program. However, this approach is only suitable for considering specific design changes for a system or device already in existence. Or, alternatively, evaluating potential CIE solutions designed to address specific cyber-attack of concern. Unfortunately, this approach is insufficient to calculate the potential returns from a CIE program implemented early in the conceptual design system of a system or device.

[6] Wilson, Bradley, Mark Arena, Lauren Mayer, Chad Heitzenrater, Jason Mastbaum, and Kevin Connolly. "A Methodology for Quantifying the Value of Cybersecurity Investments in the Navy." RAND, n.d.
[7] Magnusson, Christer, Josef Molvidsson, and Sven Zetterqvist. "Value Creation and Return On Security Investments (ROSI)," 2007. https://opendl.ifip-tc6.org/db/conf/sec/sec2007/MagnussonMZ07.pdf.

Table 2. Option 1 Strengths and Weaknesses/Gaps.

Strengths	Weaknesses/Gaps
Cost of implementation is relatively easy to calculate, particularly after implementation	Analysis focuses on a single adverse event (and approaches to mitigate it)
	May not consider the full value of implementation of CIE Principles (some principles relate to intrinsic, difficult to measure aspects, i.e., the full benefit is difficult to calculate)
	ROI-based approaches cannot be calculated for solutions that protect against unknown, undefined, or unevaluated attacks/worst case scenarios (because the effectiveness of a solution cannot be measured in the abstract)

3.2. Option #2: Consequence or Impact Reduction Following a Cyber-Attack

Hypothesis

Implementation and adoption of CIE reduces the cost of recovery in the event of a cyber-attack, incident, or other disruptive event.

Alternatively, describing the value of CIE adoption can be articulated in reduced costs associated with response and recovery actions following a cyber-attack. In this case, the hypothesis is that implementation of CIE reduces both easily measurable aspects following a cyber-attack (e.g., material/equipment replacement costs, labor hours for configuration, etc.), as well as more intrinsic "pain" that is introduced and difficult to quantify (e.g., stress applied to staff working overtime to address a security event). As noted by Suh and Han, properly calculating the risk from a disruptive event requires a systemic approach, and one in which both quantitative (e.g., material losses) and qualitative metrics (e.g., business disruptions and inefficiencies) are used.[8] (A depiction of potential losses following cyber events is included in Figure 1).

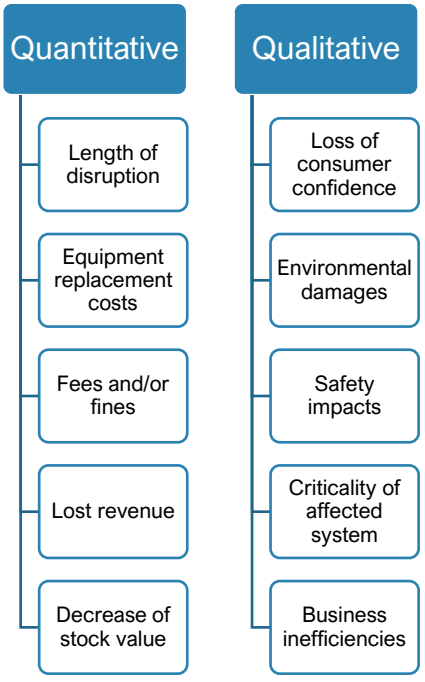


Figure 1. A figure depicting the potential effects of an adverse cyber event.

[8] Suh, Bomil, and Ingoo Han. "The IS Risk Analysis Based on a Business Model." *Information and Management* 41 (2003): 149–58.

One primary advantage to this approach is a body of research and other methodologies designed to calculate the impact of a cyber-attack, including Consequence-driven Cyber-informed Engineering (CCE). CCE enables the identification of cyber-attack impacts through a semi-quantitative approach within Phase 1 of CCE, *Consequence Prioritization*.[9] Other research promotes a similar approach. For example, Tatar et al. identify several observables to assess the disruption of cyber-attacks against an electric utility including loss of load expectancy, duration of interruption, and load curtailed per interruption (among others).[10]

POTENTIAL METHOD FOR MEASURING CIE SUCCESS

MITRE researchers identified two approaches for measuring consequence reduction. First, the CIE team could solicit input from CIE stakeholders/adoptees and others, with the goal of measuring the relative impact following a cyber event. These could be compared against average losses assessed for organizations of similar size, or against an organization that experienced a similar event. In 2020, CISA released a report summarizing their findings regarding the average cost of a cyber event, which was compiled from various insurance and consulting sources.[11] Theoretically, an asset owner/operator (or INL researchers) could compare losses or damages for CIE adoptees against these values; however, such an approach would require significant information from the CIE adoptee on the cost of CIE investments and/or mitigations. Additionally, MITRE anticipates that this approach would likely require significant assumptions about past failures or cybersecurity investments, which may weaken the strength of any CIE benefits calculation.

The best case for implementing this approach would be if INL is able to identify a single organization that has experienced a significant cyber event in the past (and has calculated its associated losses), adopted CIE principles for implementation (and calculated their cost and value), and then had a similar cyber event (after CIE adoption) to compare against.

---

[9] Freeman, Sarah, Curtis St. Michel, and Nathan Hill Johnson. "CCE Phase 1: Consequence Prioritization (Technical Report) | OSTI.GOV," May 5, 2020. https://www.osti.gov/biblio/1617458.

[10] Tatar, Unal, Hayretdin Bahsi, and Adrian Gheorghe. "Impact Assessment of Cyber Attacks: A Quantification Study on Power Generation Systems | IEEE Conference Publication | IEEE Xplore." In *2016 11th System of Systems Engineering Conference (SoSE)*. Kongsberg, Norway: IEEE, 2016. https://ieeexplore.ieee.org/abstract/document/7542959/authors#authors.

[11] "Cost of a Cyber Incident: Systematic Reivew and Cross-Validation." Cybersecurity & Infrastructure Security Agency (CISA), October 26, 2020. https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf.

Table 3. Option 2 Strengths and Weakness/Gaps.

Strengths	Weaknesses/Gaps
Direct losses stemming from a cyber-attack are easily measurable	CIE value calculations require a control for comparison (i.e., financial loss information from organizations that have implemented CIE versus those that have not)
CCE and others have developed methods to measure more intrinsic (qualitative) damages associated with cyber events/attacks	Requires a cyber event or incident to measure against (rather than a comparison against normal operational costs)

3.3. Option #3: Reducing Security Costs through Proactive Investment

Hypothesis

Proactive security investment, based on CIE, costs less and is more effective than reactive security policy implementation following a cyber incident.

As noted by a representative of the UK-based cybersecurity firm NCC Group:

> *[Although] there are many claims that [cybersecurity] is an indispensable necessary cost, there is also a body of opinion that [cybersecurity] does not always justify its costs and the costs of a breach are frequently either exaggerated or unclear.*[12]

The above quotation perfectly expresses the sense of skepticism that often plagues security budget requests. This feeling is acute in resource constrained environments, where dollars appropriated for proactive defense may be taken from budgets for other pressing concerns. However, there has long been the belief that investments ahead of a crisis are more cost effective than those during or after, and limited data indicates that the same logic should be applied to cybersecurity investments. In fact, a common axiom is "A one dollar investment to manage a bug in the designing process will save $99 compared to managing a bug later in the implementation phase." This perspective was manifested in the Hoover model, developed by the Massachusetts Institute of Technology (MIT) in partnership with the Boston-based company, @Stake. Findings of that model cautioned against adding in security at the end of development, noting that the earlier one implements security into the software design process, the higher the investment yield. The highest returns, 21 percent, were achieved for investments in the

[12] Dunn, Nick. "The Economics of Defensive Security." NCC Group, 2018. https://research.nccgroup.com/wp-content/uploads/2020/07/ncc-group-whitepaper-the-economics-of-defensive-security.pdf.

development phase, as compared to 15 percent returns in the implementation phase and 12 percent returns in the testing phase.[13]

In 2014, Kwon and Johnson observed similar trends within the healthcare sector, noting that the cost between proactive and reactive investment varied significantly (e.g., adoption of data protection methods for electronic medical records with average costs of proactive implementation (~$1.6M) versus following an incident (~$11.3M)).[14] Additionally, Kwon and Johnson determined that the effectiveness of security solutions also faltered when adopting a reactive approach. They theorized that this may be a result of the fact that reactive security approaches may involve the adoption of "myopic bug chasing" or overly focusing on "obsolete threats."[15] Considering CIE, these findings are significant as they suggest the core value of CIE is in its early adoption, either early in the product lifecycle or ahead of an attack, incident, or other disruptive cyber event.

POTENTIAL METHOD FOR MEASURING CIE SUCCESS

Through a review of existing approaches, MITRE researchers identified two scenarios in which measuring the financial benefits of CIE adoption is beneficial. First, considering regulated or otherwise required security investments, early adoption of CIE principles reduces the cost of security activities. Second, implementing security requirements ahead of a breach or security event can reduce the overall cost associated with implementing improved security. In both cases, the two categories of investment (i.e. proactive versus reactive) can be compared (Figure 2) to demonstrate the reduced cost of CIE adoption.

Figure 2. Proactive versus reactive costs when responding to a cyber event.

Proactive Investment	Reactive Investment
• Initial investment in solution/approach • Ongoing operational cost (efficiency of security operations • Monitoring and/or compliance costs • Enables more efficient identification (and funding of) suplemental security services • Opportunity to identify and eliminate unnecessy or redundant solutions or services	• Cost to implement required mitigation -or- the cost associated with incident response activities • Recovery costs (if applicable) • Cost of fines or fees (if applicable) • Impact to reputation or consumer confidence (if applicable)

Similar to Option #2 above, this calculation would require a control or base value against which to compare. This comparison is most easily performed with actual, negative repercussions following an adverse event (e.g., cost to bring a system into compliance following an audit, associated fines for lack of compliance, costs associated maintenance and servicing), rather

---

[13] Magnusson, Christer, Josef Molvidsson, and Sven Zetterqvist. "Value Creation and Return On Security Investments (ROSI)," 2007. https://opendl.ifip-tc6.org/db/conf/sec/sec2007/MagnussonMZ07.pdf.

[14] Kwon, Juhee, and M. Eric Johnson. "Proactive Versus Reactive Security Investments in the Healthcare Sector." *MIS Quarterly* 38, no. 2 (June 2014): 451–72.

[15] Kwon, Juhee, and M. Eric Johnson. "Proactive Versus Reactive Security Investments in the Healthcare Sector." *MIS Quarterly* 38, no. 2 (June 2014): 451–72.

than theoretical outcomes. Using theoretical data, as is the case in Option #2, may result in a collision of these two approaches but enables a comparison to be made between proactive and reactive investment without requiring an adverse event. (The primary difference between Option #2 and Option #3, is that Option #2 is designed to consider quantitative and qualitative values, while Option #3 is focused on (relatively) easily quantifiable items (i.e., financials)).

Table 4. Option 3 Strengths and Weakness/Gaps.

Strengths	Weaknesses/Gaps
Easily quantifiable measurement (e.g., cost of security investment)	No easily identified 'control' to measure against
	Requires participation/support from an asset owner/operator that has implemented CIE
	Does not consider the full security 'value' provided by CIE adoption

3.4. Option #4: Addressing Organizational Susceptibility to Cyber-Attacks

Hypothesis

CIE reduces the attack service of the CPS to which it is applied, and in doing so reduces the susceptibility of these systems to specific attacks.

An alternative option would be to consider the susceptibility of a specific system or component before and after CIE implementation. Susceptibility is a construct that considers both adversary capabilities as well as defender capacity to protect a system. In this regard, susceptibility is akin to but distinct from attack surface analysis.

Susceptibility of CPS systems is measured as a part of MITRE's Infrastructure Susceptibility Analysis (ISA).[16] This approach enables organizations to evaluate the susceptibility of their CPS before and after specific mitigations are enacted. ISA is designed to inform mitigation efforts, guaranteeing that organizations apply defensive and engineering-based mitigations (i.e., modifications to CPS design) in the locations of greatest risk. This ensures that limited resources are applied most effectively.

Similarly, CIE solutions (and associated metrics) could be designed to measure the reduction potential impact following an adverse event (and therefore a reduction in risk or susceptibility) that emerges as a result of CIE implementation. Key to this approach, however, is a thorough understanding of the threat environment, the capabilities and intentions of threat actors, and the limitations of the adversary's offensive cyber programs. Currently, this kind of threat intelligence approach is outside of the scope of CIE application. Alternatively, CIE metrics could be designed to measure the reduced attack surface that emerges following the application of CIE principles.

[16] "Infrastructure Susceptibility Analysis and Assessments | MITRE." Accessed September 17, 2024. https://www.mitre.org/news-insights/fact-sheet/infrastructure-susceptibility-analysis-and-assessments.

However, given the lack of consensus associated with attack surface quantification, MITRE is not recommending this option for integration into CIE benefits quantification at this time.

3.5. Option #5: Measuring "Future-Proofing" Critical Infrastructure

The true value of CIE stems from the opportunity for introspection it affords organizations. Application of CIE principles ensure organizations review potential risks, both cyber-induced and 'natural,' in a structured way. This can increase the confidence of C-suite and leadership as they make decisions and plan strategies around tolerable risk. Leadership is better able to understand their greatest weaknesses, where contingency plans are constrained, and where their ability to transfer unacceptable risk is limited. Although some may equate this to the increased resiliency of CPS, the true gains of CIE originate from understanding the risk (and effects/impacts) of CPS failures to inform decisions to improve resiliency. Ultimately, CIE is a combination of introspection, with some degree of validation, on the way to cybersecurity determinism (e.g., secure-by-design).

Unfortunately, the complexity surrounding the true value of CIE limits the applicability of existing approaches. Because of this, MITRE investigated the design of a custom scale to measure the maturity of CIE Principle adoption either across an organization or considering a specific system design.[17] This custom scale is included in Table 5. Although still in draft form, this scale provides a path to measure the ability of a system or organization to resist future, even yet unidentified, attacks. In this way, the scale is designed to measure a kind of cybersecurity "armor class,"[18] and serves a measurement of the degree of future-proofing present in a system or organization.

PROPOSED METHOD FOR MEASURING CIE SUCCESS

As mentioned above, Table 5 is designed to evaluate the degree of CIE adoption by a given organization. This could be summarized as a "CIE Maturity Level" scale; however, this arguably belittles the full spectrum of CIE adoption benefits. Described another way, the value of CIE adoption extends beyond a simple CIE "score" but instead addresses the ability of an organization to repel future attacks through the commissioning of resilient CPS and preparation of an organization's engineers, developers, designers and other staff. In this instance, CIE bolsters the technology, people, and processes against adverse cyber events, reducing the severity/consequence of an event, the cost and time required for restoration, and decreasing the frequency of adverse cyber events over time.

MITRE considered two primary use cases for the application of the Likert scale defined in Table 5: evaluation of ***existing*** or ***future*** device(s), system(s), or program(s) against CIE implementation principals. In either case (existing or future), the process follows a similar path (Figure 3). If desired, the organization could also leverage the draft metrics in Table 5 to perform

[17] (It should be noted that the "Metrics" column includes theoretically possible, 'first cut' metrics; however, several are likely impractical given the assumptions they require. MITRE included these to encourage follow-on discussions to better frame potential metrics.)

[18] Armor class (AC) represents a numerical representation of a character's defense in the roleplaying game, Dungeons & Dragons (D&D). AC combines a character's active (e.g., ability to avoid a hit, etc.) and passive defenses (e.g., strength of armor, etc.). Higher AC are more desirable and reduce the likelihood that a given attack will do damage.

trend analysis over time; in this case, CIE "success" is defined as an increase in positive elements/instances (e.g., number of high quality high-consequence events (or equivalent) documented against each critical function) and a reduction of negative (i.e. detrimental) elements/instances (e.g., quantity of business sensitive information stored on third-party systems or networks). In this case, it is critical that the organization review the potential metrics and modify, reject, or adopt as it aligns with their priorities and risk posture. The organization must reach concurrence on the most relevant metrics prior to collecting and analyzing data to support long term trend analysis.

The method defined in Figure 3 is summarized in the following equations:

$$CIE_i = \sum \alpha(CPS_a) + \beta(CPS_{b)} \ldots$$

$$CIE_x = \sum \alpha(CPS_a) + \beta(CPS_{b)} \ldots$$

$$CAC_x = (CIE_i - CIE_x)$$

$where,$

$CIE_i = Initial\ CIE\ implementation\ score$

$CIE_x = CIE\ implementation\ score\ following\ mitigation\ plan$

$CAC = Cybersecurity\ Armor\ Class\ (following\ x\ implementation\ plan)$

Figure 3. Method for Measuring CIE Adoption Levels.

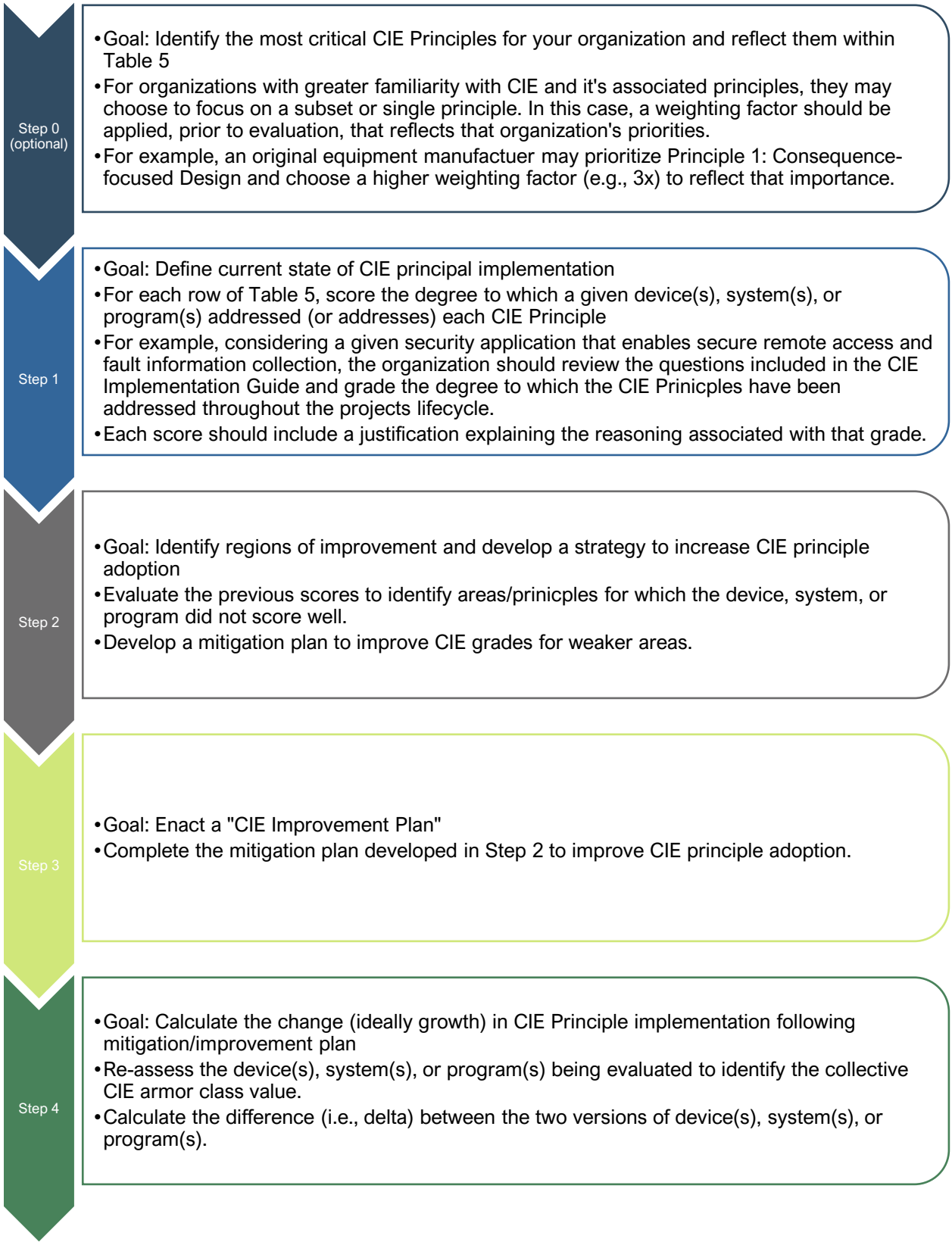


Table 5. Scale to Measure CIE Adoption Levels.

CIE Principle	Goal	Potential Metrics	Low (1)	Medium (3)	High (5)
1 Consequence-Focused Design	Organization has considered high-consequence events, system failures or the equivalent. Analysis could be conducted as part of mission/business assurance, Crown Jewel Analysis, Phase I CCE, or something else.	Number of critical functions identified and documented. Number and quality of high-consequence events (or equivalent) documented against each critical function. Percentage of critical functions that have had their failure modes assessed.	The organization has not considered the worst-case outcomes that could result from cyber-attacks. The organization has minimal understanding of its critical functions. No formal processes are in place to identify and prevent undesired consequences. Cyber-related consequences are largely unrecognized or ignored in system design and operational planning.	The organization has reviewed past cyber-attacks but may not have considered the severity of the attack's consequences if applied against their own systems. The organization has identified some critical functions but may not have fully mapped all potential consequences of failure. Alternatively, the organization may have considered the consequences of their design in the original deployment and design of the system but may not return to review the implications of future modifications and/or updates. There are processes in place to address some risks, but they may not cover all critical systems or phases. Cybersecurity and consequence-focused strategies are applied inconsistently, and there are gaps in addressing cyber-enabled risks across systems.	The organization has a well-documented and structured process to identify all critical functions and the undesired consequences of their failure. Detailed consequence assessments are integrated into all phases of system design, development, and operation. The organization continues to review the system (and its associated critical functions) over time, as the system evolves, new functionality is added (or removed), and the architecture changes. Cybersecurity strategies and engineered controls (where applicable) are consistently implemented to mitigate identified risks/consequences, with regular reviews and updates ensuring resilience.

CIE Principle	Goal	Potential Metrics	Low (1)	Medium (3)	High (5)
2 Engineered Controls	Implement physical and digital engineering controls that can reduce or eliminate cyber risks, minimizing the reliance on post-design IT security measures.	Percentage of critical systems covered by engineered physical or operational controls. Number of diverse engineered controls to reduce adversary opportunities.	The organization has integrated some engineered controls into system design, but those controls have not been reviewed to ensure "survivability" in the event of a malicious and intelligent cyber actor. Engineering staff have not considered how an adversary could use the compromised system (as designed and engineered) to achieve a malicious outcome. Reliance is primarily on post-design IT or other security controls, with no focus on eliminating or mitigating attack vectors through physical or operational engineering. Cybersecurity is an afterthought and considered primarily after the final design is set.	The organization has implemented some engineered (non-cyber) controls, but they are not consistently applied across all critical systems. Engineering teams have made some modifications to reduce avenues for attack, but there are still significant gaps where digital systems are vulnerable. There is collaboration between cybersecurity and engineering teams, but the integration of cyber controls beyond the early design phases is partial or inconsistent.	Engineered controls are fully integrated into the earliest stages of system design, with specific attention given to eliminating or minimizing attack vectors. Additionally, engineered controls are reviewed and validated for effectiveness following implementation or modification to the system design, functionality, or architecture. Engineering decisions and modifications are made with the explicit goal of reducing opportunities for the adversary in the event of compromise, using non-digital controls where appropriate, to limit system exploitability. Collaboration between engineering and cybersecurity teams is comprehensive, ensuring that physical and cyber controls work together to protect against attacks from the outset and through the system lifecycle.

CIE Principle	Goal	Potential Metrics	Low (1)	Medium (3)	High (5)
3 Secure Information Architecture	Structure and secure data to prevent unauthorized access or manipulation, focusing on critical data exchanges that are essential to system safety and operation.	Quantity of critical data stored outside of system security boundaries. Number of shared accounts used in the system. Number of third-party managed service providers that have access to critical data. Percentage of system-to-system accounts that have not been set to least privileged.	The organization has minimal segregation of critical data and systems, with no clear information architecture to protect sensitive information. Data transmission and storage lack encryption or access controls, and there is no formal process for managing or securing data across systems. Security measures for data integrity, confidentiality, and availability are either absent or inconsistently applied, making critical systems vulnerable to manipulation.	The organization has implemented basic security measures, such as some encryption and access controls, but these are not systematically applied across all data streams and systems. There are processes to protect critical data, but they may not be comprehensive or fully integrated into system architecture. For example, individuals (e.g., employees, contractors) go through an initial background screening to ensure trustworthiness. The organization is aware of data integrity risks and has some measures in place (such as backups of some critical data stores), but the security architecture still lacks full resilience against potential cyber threats or manipulation. The organization may place unverified trust in third-party organizations that offer data protection/backup services or grant access to critical data flows as part of a managed service.	The organization has fully implemented a secure information architecture, with robust segregation of critical data and systems to ensure controlled access, monitoring, and protection. The robustness of this design has been validated, for example through third-party penetration testing, reverse engineering, vulnerability assessments, or other reviews. Encryption, access controls, and data validation mechanisms are consistently applied across all data streams, ensuring data confidentiality, integrity, and availability. Data access and data control is based on individual roles, and those accesses are periodically reviewed to ensure they continue to align with job duties and functions. The architecture is proactive in preventing unauthorized manipulation of data, with continuous monitoring and layered defenses integrated into every phase of system design and operation, ensuring resilience against both internal and external threats. Critical data sources and storage have been identified, are protected with the highest security controls, and maintained, controlled, and stored within the organization's own systems.

CIE Principle	Goal	Potential Metrics	Low (1)	Medium (3)	High (5)
4 Design Simplification	Eliminate unnecessary features and reduce system complexity to minimize cyber vulnerabilities and ensure only essential functions are incorporated.	Reduction in system complexity (number of unnecessary components/functions removed). Percentage of systems with documented simplification efforts. Reduction in failure rate due to simplification. Reduction in maintenance due to simplification.	The organization has not prioritized simplification in its system design, leading to excessive complexity with unnecessary digital features or components. The system includes many functions or features that are not critical to its primary purpose, increasing the attack surface and operational risks. There is little to no effort to identify or eliminate latent capabilities that could be exploited by adversaries, and no simplification of system architecture to reduce risk.	Some effort has been made to simplify the design, with the organization removing or minimizing a few non-essential features. The system's complexity is somewhat reduced, but there are still components or capabilities that could be streamlined to better align with security and operational goals. The organization is aware of the risks posed by unnecessary complexity, but the design still includes features that are not strictly required for critical functions, leaving some potential vulnerabilities.	The organization has fully embraced design simplification, ensuring that the system includes only the features and functions necessary to achieve its critical objectives. Non-essential features and latent digital capabilities that could increase the system's complexity or vulnerability have been identified and removed or neutralized. The system is designed for operational simplicity, reducing potential attack surfaces and creating a more resilient, streamlined architecture, while maintaining all necessary functionality and security.
5 Layered Defenses	Apply multiple defensive layers (e.g., diversity, redundancy) to mitigate potential failures and ensure system resilience, even under cyber-attack.	Quantity (number of) of diverse defense solutions. Percentage of systems with redundant critical components.	The organization has implemented few or no layers of defense, relying heavily on a single security solution (e.g., firewall or antivirus) without redundancy. There is no clear strategy for mitigating cascading failures or containing threats once they penetrate the system. Defensive measures are inconsistent, leaving critical functions exposed to single points of failure or compromise.	The organization has implemented some layered defenses, but the approach may lack coordination or full coverage across all critical systems. There are redundant controls in place, but they do not cover all areas of potential vulnerability, and there are still opportunities for cascading failures. The defense strategy includes some monitoring and response mechanisms, but they are not fully integrated to provide a cohesive, multi-layered security architecture.	The organization has fully implemented a defense-in-depth strategy, with multiple layers of physical, digital, and operational controls working together to protect critical functions. Redundant systems and controls are in place, ensuring that the failure or compromise of one layer does not lead to the failure of the entire system. The layered defenses include active monitoring, automated response mechanisms, and proactive measures to detect, contain, and recover from threats, ensuring robust protection against both known and unknown risks.

CIE Principle	Goal	Potential Metrics	Low (1)	Medium (3)	High (5)
6 Active Defense	Proactively detect and respond to cyber threats through continuous monitoring and rapid response mechanisms, ensuring system defenses are dynamic and adaptable.	Percentage of systems with real-time monitoring. False positive detection rate.	The organization has no active monitoring or real-time threat detection (or similar) capabilities in place. Incident response is entirely reactive, with no preplanned contingency actions to mitigate threats before they cause significant damage. There is no real-time detection of anomalies or proactive measures to identify potential cyber threats.	The organization has implemented some real-time monitoring and anomaly detection, but these systems may not cover all critical functions or assets. (Alternatively, if an organization chooses not to implement a solution, then is the reasoning documented.). Incident response plans are in place but may not be regularly tested or updated to reflect evolving threats. There is some capacity for detecting and responding to threats in real time, but the response mechanisms may be manual or slow, limiting the organization's ability to contain threats quickly.	The organization has a fully integrated active defense system, including real-time monitoring, automated threat detection, and rapid response capabilities across all critical systems. Preplanned contingency actions are well-defined and regularly tested, allowing the organization to quickly detect, isolate, and neutralize threats before they can cause major disruptions. The defense posture is proactive, continuously evolving to meet new threats, and supported by advanced tools that can detect, analyze, and respond to cyber threats in real time, ensuring minimal disruption to critical functions.

CIE Principle	Goal	Potential Metrics	Low (1)	Medium (3)	High (5)
7 Interdependency Evaluation	Understand and manage how different systems interact, preventing cascading failures by evaluating the impact of system dependencies.	Number of identified system interdependencies, including interdependencies that exist in data, processes and technology. Percentage of systems with risk mitigation for interdependencies.	The organization has little to no awareness of the interdependencies between its systems, services, and external partners. Similarly, the organization has not considered any underpinning data or processes on which these systems may rely. There is no formal process for evaluating how the failure or disruption of one system may impact others, internally or externally. Potential cascading failures from interdependent systems are not regularly considered in risk assessments or system design.	The organization has sought to identify some interdependencies between data, processes and technologies, as well as organizational reliance on external third parties but does not have a comprehensive view. There are occasional evaluations of how disruptions in one system may affect others, but these assessments may be incomplete or reactive rather than proactive. Interdependency considerations are included in risk assessments and design processes, but the focus may be on high-profile systems, leaving others under-evaluated.	The organization has a thorough understanding of the interdependencies between its data, processes and technology (both internally and externally). Experienced staff have thought through system interdependencies and have considered a shift in procedures when core systems are unavailable. Regular, proactive evaluations are conducted to assess the potential impact of system disruptions on interdependent systems, with specific plans in place to address cascading failures. Interdependency evaluations are fully integrated into risk management, system design, and operational planning, ensuring that the organization is prepared to manage and mitigate risks from interconnected systems and services.

CIE Principle	Goal	Potential Metrics	Low (1)	Medium (3)	High (5)
8 Digital Asset Awareness	Understand how digital device adoption modifies the engineered functionality (or its survivability). After systems are deployed, organizations maintain detailed awareness of all digital components, their functions, and their potential vulnerabilities to better manage risks and defenses.	Percentage of digital assets inventoried. Number of undocumented or unapproved assets detected. Percentage of systems with real-time asset monitoring.	The organization may have adopted digital assets or automation in places without consideration for loss of availability and/or functionality. The organization lacks a clear inventory or understanding of its digital assets, with limited tracking of where digital systems, software, or data are used. There is no formal process for identifying or monitoring digital assets, leading to potential blind spots in security. Assumptions about the functionality and security of digital assets are not regularly reviewed, leaving vulnerabilities unaddressed.	Some digital device or automation adoption puts critical functions at risk; however, engineering teams have attempted to mitigate the risk associated with digital device loss or manipulation. The organization has a basic inventory of its digital assets, including some awareness of where and how they are used in critical functions, though tracking may be incomplete. There is a process in place for identifying new digital assets, but it may not be consistently enforced or updated across all departments. Regular assessments are conducted to review assumptions about digital asset functionality, though this may not cover all assets or consider evolving risks.	If digital devices have been adopted (replacing core systems and their functionality), the organization has reviewed and documented any potential risks resulting from their adoption (and has accepted that risk). The organization maintains a comprehensive, up-to-date inventory of all digital assets, with clear understanding of where each asset is used, its functionality, and its security risks. The organization may use sunsetted equipment but has a plan for replacement of these devices in the future (even if it is not complete yet). A robust process is in place to continuously track and monitor digital assets, ensuring that any new assets are immediately accounted for and integrated into security protocols. Regular, detailed assessments are conducted to evaluate assumptions about digital asset functionality, with proactive measures taken to address any potential vulnerabilities as systems evolve.

CIE Principle	Goal	Potential Metrics	Low (1)	Medium (3)	High (5)
9 Cyber-Secure Supply Chain Controls	Ensure that all third-party suppliers adhere to security standards, mitigating risks introduced through external products or services.	Quantity (or number of) supply chain controls (e.g., approved vendor list, defined requisitions in the procurement/ contracting language). Percentage of critical components sourced from secure suppliers.	The organization has not considered cybersecurity or has an extremely nascent program in development, in which they have only considered the implications of supply chain attacks. Similarly, the organization has not integrated any formal processes or controls to secure the supply chain from cyber threats. There are little to no security requirements are set for suppliers (or the security controls are insignificant in their ability to proactively protect the organization), and there is little to no verification of the security posture of vendors (third-party or otherwise). In general, there is limited awareness or understanding of the cybersecurity risks associated with the supply chain.	The organization has established some baseline cyber-secure supply chain controls, such as procurement language that promotes cybersecurity standards and defined requirements for suppliers regarding cybersecurity. Cybersecurity or other assessments are conducted periodically to evaluate the risk from supply chain vectors; however, this kind of review may not be comprehensive or enforced consistently across all suppliers. The organization has implemented some security controls, but some identified risks related to supply chain vulnerabilities remain unaddressed, primarily due to resource constraints or other similar barriers.	The organization has fully integrated and enforced a comprehensive set of cyber-secure supply chain controls, including rigorous vendor requirements, regular security assessments, and audits. The organization has established a transparent relationship with key suppliers, and communications are robust and frequent between the two organizations. Suppliers admit if they face challenges that may affect the ability of the supplier to meet contract needs, as well as inform the organization of any potential cyber incidents/events promptly. The organization continuously monitors supply chain risks and/or vulnerabilities, and vendors are required to meet stringent cybersecurity standards. This monitoring activity is paired with robust solutions and/or frameworks for detecting, responding to, and mitigating risks, vulnerabilities, or potential consequences of cyber attacks.

CIE Principle	Goal	Potential Metrics	Low (1)	Medium (3)	High (5)
10 Planned Resilience	Design systems to anticipate failure, ensuring they can continue functioning (or fail safely) even during a cyber-attack or technical fault.	Percentage of systems with restoration plans. Number of restoration exercises per year. Percentage of system backups that are tested.	The organization has few, if any, formal plans or processes for maintaining system functionality in the event of cyber disruptions or failures. Recovery processes are largely reactive, with little to no anticipation of potential cyber threats or resilience measures. Redundancies, backups, or contingency planning are minimal or nonexistent, leaving critical functions vulnerable to failure.	Some planned resilience strategies are in place, with recovery procedures for certain cyber incidents, though they may not cover all critical systems or functions. The organization has identified potential cyber risks and has implemented basic measures, such as backups or failovers, but resilience planning may not be fully integrated into the design process. There are documented recovery processes, but they may be inconsistently tested or updated, and not all personnel are fully aware of their roles during an incident.	The organization has a well-developed, proactive resilience plan that covers all critical systems and functions, anticipating a wide range of cyber threats and disruptions. Resilience is integrated into system design from the outset, with robust redundancies, failovers, and recovery mechanisms designed to ensure continuous operation during and after cyber incidents. Regular training, testing, and updating of resilience plans are part of the organizational culture, ensuring that all personnel understand their roles and that the organization can swiftly recover from disruptions without significant impact. Training includes methods for operating without core critical control systems.

CIE Principle	Goal	Potential Metrics	Low (1)	Medium (3)	High (5)
11 Engineering Information Control	Protect sensitive engineering information from unauthorized access and misuse, ensuring that critical system knowledge remains secure.	Percentage of critical engineering documents with access restrictions. Time to revoke access to sensitive engineering information. Percentage of data stores whose users are reviewed annually.	Limited controls are in place for managing and protecting engineering information. Access to sensitive engineering data is poorly regulated, and there are no clear protocols to prevent unauthorized access or sharing. There is little to no training or awareness regarding the importance of safeguarding engineering data, leading to potential security risks.	Engineering information control processes exist but are inconsistently applied across the organization. Some measures are in place to control access to sensitive engineering data, though they may not be well enforced or monitored regularly. Employees are somewhat aware of the importance of protecting engineering data, with basic training and guidelines available but not universally followed.	The organization has robust, well-documented controls in place for managing and protecting engineering information at all stages of the system lifecycle. Access to engineering data is tightly controlled, regularly monitored, and limited to authorized personnel, with clear protocols for handling, sharing, and storing information. A culture of vigilance regarding information control is embedded in the organization, with regular training, strict enforcement, and a proactive approach to protecting sensitive engineering data from unauthorized access or manipulation.
12 Organizational Culture	Foster a culture where all personnel are aligned with cybersecurity goals, ensuring that behavior and decision-making consistently support system security and resilience.	Number of business units involved with cybersecurity policy review. Percentage of implementation team that have gone through cybersecurity training.	Cybersecurity is seen as the sole responsibility of IT or cybersecurity teams, with little to no integration into engineering or other business units. There is limited awareness or engagement with cybersecurity practices among non-cyber staff. Cybersecurity considerations are reactive, with no emphasis on a proactive, security-focused culture throughout the organization.	Some organizational units beyond IT are involved in cybersecurity practices, but collaboration is inconsistent. Cybersecurity awareness is promoted, and some training programs are in place, though engagement varies by department. Security considerations are becoming integrated into the decision-making processes, but not uniformly across the organization.	A robust, organization-wide culture of cybersecurity exists, with collaboration across engineering, IT, and business units. Cybersecurity is integrated into the daily responsibilities of all employees, supported by comprehensive training and regular updates. Leadership consistently emphasizes and models a proactive security mindset, ensuring that security considerations are aligned with all aspects of the organization's operations and decision-making.

4. Recommended Path Forward

As mentioned above, the CIE team seeks to develop an approach that defines the value of CIE implementation, along with suitable metrics, to:

- Measure CIE implementation success elements and outcomes;
- Identify (and calculate) the value from early adoption of CIE; and,
- Determine (and calculate) the business justification for CIE implementation, especially on existing infrastructure.

MITRE researchers evaluated several techniques that are currently used to prioritize business investments in cybersecurity or to calculate the returns on past cybersecurity investments. Additionally, MITRE also considered the limitations of these approaches, including, but not limited to, potential challenges with acquiring the necessary data for calculations and the difficulty associated with articulating the intrinsic benefits of CIE adoption. Ultimately, the MITRE team determined that there is no existing approach for cybersecurity metrics that is suitable for all cases to which the CIE program seeks to apply it. Instead, CIE must adopt and modify existing approaches to determine their utility and effectiveness.

In support of this quest, MITRE recommends that CIE continue to evaluate the utility of the custom measurement tool included in Table 5. For example, the comprehensiveness of the Likert scale could be improved through targeted interviews with CIE stakeholders and adoptees, validating the completeness of the current scale. Similarly, this scale should also be applied in specific use cases to determine the effectiveness of this tool in comparing various CIE-inspired systems or programs.

Finally, it should be noted that several sector-specific strategies and approaches exist to address cybersecurity risks and/or reduce the impact of adverse cyber-events. Complete evaluation of these approaches is outside of the scope for this document. Ultimately, individual sectors and/or sector-specific organizations must define a scale that aligns with their goals and needs.

5. Acronyms

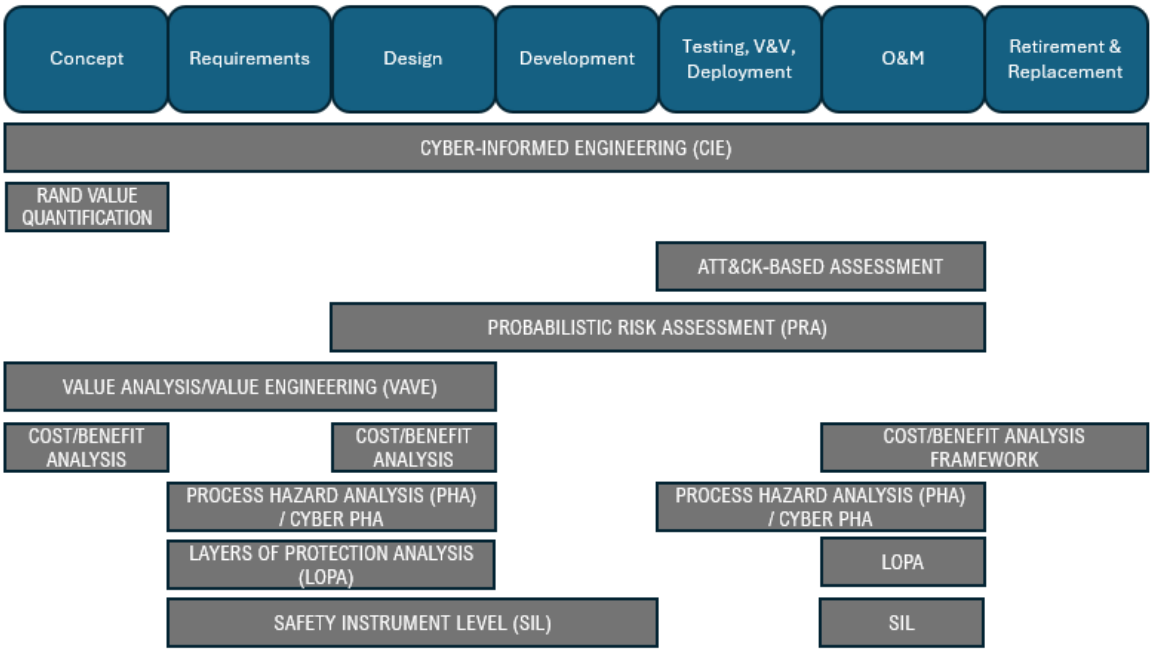
CCE	Consequence-driven Cyber-informed Engineering
CF	Contact frequency
CIE	Cyber-informed Engineering
CISA	Cybersecurity and Infrastructure Security Agency
CoA	Courses of Action
CPS	cyber-physical system
CVaR	Cyber Value-at-Risk
DOE	Department of Energy
FAIR	Factor Analysis of Information Risk
INL	Idaho National Laboratory
IPL	Independent Protection Layers
ISA	Infrastructure Susceptibility Analysis
IT	Information technology
LEF	Loss Event Frequency
LM	Loss Magnitude
LOPA	Layers of Protection Analysis
MIT	Massachusetts Institute of Technology
NREL	National Renewable Energy Laboratory
PoA	Probability of action
ROI	return on investment
RS	Resistance strength
SL	Secondary Loss
SBOM	Software bill of materials
TCap	Threat capability
VaR	Value at Risk
Vul	Vulnerabilities
PL	Primary Loss
PFD	Probability of Failure on Demand

Appendix A: Evaluated Analytic Methodologies

MITRE researchers considered a variety of existing approaches to: 1) prioritize security investments, 2) conduct cost-benefit analysis on expenditures, and 3) understand the value added for those activities. The goal of this review was to determine what existing approaches have been adopted by the broader security community and to determine if any were appropriate for modification for calculating CIE value. Included in this appendix is a subset of those analytic methodologies reviewed.

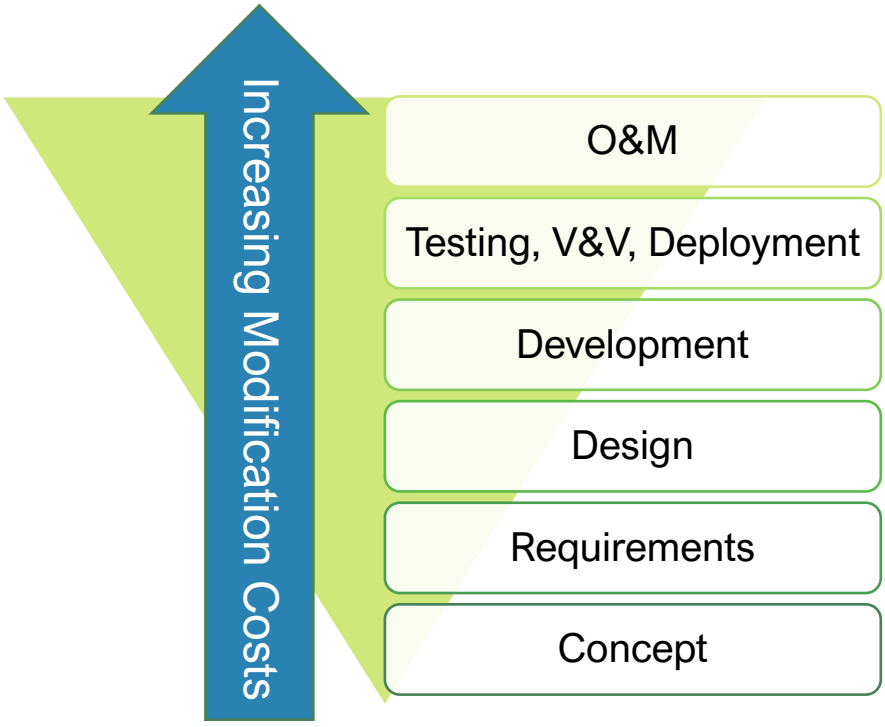
Interestingly, a review of multiple approaches identified a dichotomy between the various lifecycle phases. Approaches exist for evaluating future (i.e., conceptual systems), as well as modifications of existing systems; however, MITRE researchers failed to identify a single approach that could be applied throughout the lifecycle, from earliest concepts to testing to commissioning to retirement (Figure 4). CIE is unique in its applicability to and ability to address potential cyber risk throughout the CPS lifecycle.

Figure 4. Reviewed Methodology Applicability by Design Phase.



Additionally, it has been proposed that adoption of CIE principles have the greatest returns when applied in the earliest stages of conceptual design and requirements development. Early application not only increases the efficacy of CIE-inspired modifications, but it can also significantly reduce the cost of modifications. In contrast, requesting modifications of a system after it has been commissioned requires significant investment (Figure 5).

Figure 5. Anticipated increasing costs of system/device modification against the CPS lifecycle.

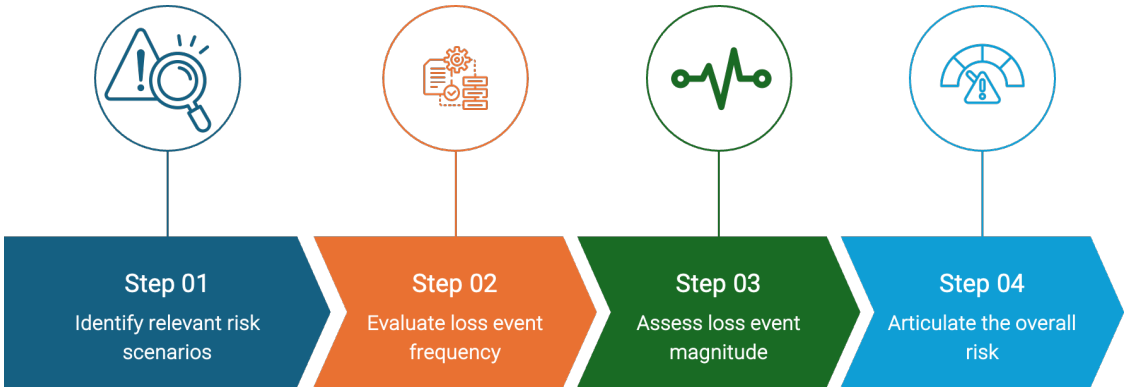


A.1 Factor Analysis of Information Risk (FAIR)

FAIR™ (Factor Analysis of Information Risk) provides a detailed model for understanding, analyzing, and quantifying cyber and operational risks in financial terms.[19] Unlike traditional risk assessment methods that use qualitative charts or weighted scales, FAIR translates risk into monetary values. This enables a solid foundation to convert these risk estimates into potential financial loss and incorporate them into an organization's existing business processes.

[19] "The Importance and Effectiveness of Cyber Risk Quantification." Accessed September 17, 2024. https://www.fairinstitute.org/what-is-fair.

Figure 6. A high-level depiction of the FAIR methodology.



The FAIR cyber risk analysis process includes four steps (Figure 6). This structured approach helps organizations systematically identify potential threats, estimate their likelihood and impact, and calculate the financial risk involved. Central to the FAIR process are *Loss Event Frequency (LEF)* and *Loss Magnitude (LM)*, summarized below:

- **Loss Event Frequency (LEF):** Determined by factors like *Threat Event Frequency (TEF)* and Vulnerabilities (Vul), further influenced by *Contact Frequency (CF)*, *Probability of Action (PoA)*, *Threat Capability (TCap)*, and *Resistance Strength (RS)*. These factors help quantify how often a threat might occur and the likelihood of it leading to a loss.
- **Loss Magnitude (LM):** Divided into *Primary Loss (PL)* and *Secondary Loss (SL)*, it captures the direct and indirect financial impacts of a threat.

Using these factors, risk to the organization can be calculated using the following equation:

$$\text{Risk} = (\text{CF} * \text{PoA}) \left(\frac{\text{TCap}}{\text{RS}}\right) (\text{PL} + \text{SL})$$

Table 6. FAIR Strengths and Weaknesses/Gaps.

Strengths	Weaknesses/Gaps
Approach is well documented in publicly accessible resources	Model focuses on financial loss but fails to calculate the cost of solutions or continued operations and maintenance associated with solutions
Supports combined calculations that consider both existing costs and perspective costs (e.g. cost can't be realized until an incident occurs)	Not easily generalizable across a sector or industry as calculations are based on assumptions that are unique to an organization
If interested, organizations can create Monte-Carlo simulations (or similar tools) to estimate qualitative costs (provided sufficient data exists	Efforts to model potential losses (such as through Monte-Carlo simulations) requires substantial high-quality data, such as failure frequency for relevant CPS
Underlying framework supports the mapping of controls and defenses similar to the ATT&CK model	Measurement of loss, vulnerability, and effectiveness is difficult

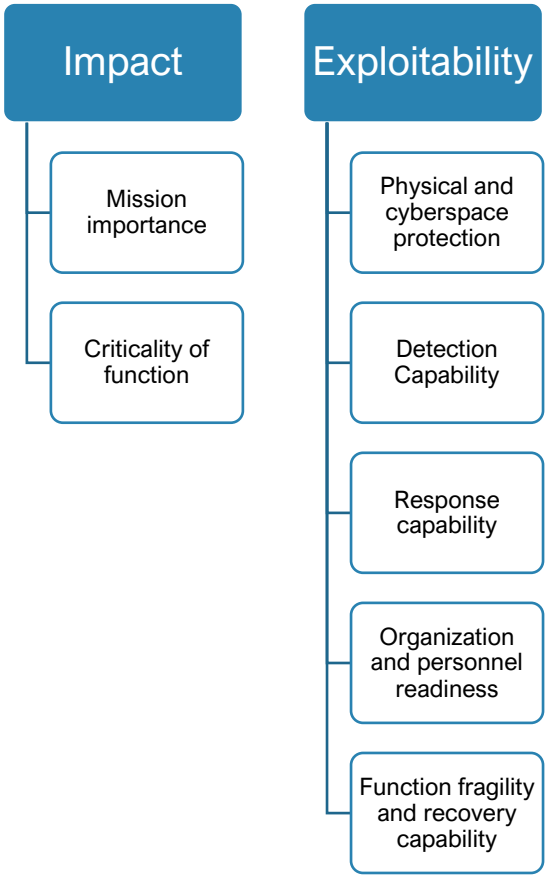
Ability to Calculate CIE Value

Notionally, it may be possible to co-opt aspects of the FAIR calculation (or a similar calculation) to measure and track a reduction in the frequency of adverse events or naturally occurring system failures following CIE implementation. The data requirements for this approach, however, are extremely high and may not be worth the level of investment requires to compile and maintain the associated data set.

RAND VALUE QUANTIFICATION METHODOLOGY

In 2022, RAND published its Value Quantification Methodology, which seeks to prioritize proposed Target(s) of Investment (TOI) for Department of Defense (DoD) investment. RAND's approach requires a review of two components (impact and exploitability) and can be decomposed into several factors (Figure 7).

Figure 7. Core aspects of RAND's Value Quantification process.



Each factor has a predefined scale from 1 to 5, with definitions for each rating. The following formula is used to calculate the TOI's impact:

$$Impact = \max\ (\text{Mission Importance}, \text{Criticality of function})$$

OR

$$Impact = \text{average}\ (\text{Mission Importance}, \text{Criticality of function})$$

To calculate the TOI's exploitability, analysts first rate each facet without the TOI implemented (staring exploitable factor) and then with the TOI implemented (final exploitable factor). Analysts can then calculate the reduction (or delta) of the exploitable factor due to the TOI. Taking the sum of the applicable deltas, analysts then calculate the Exploitability Reduction Effectiveness (ERE) using the following formula:

$$ERE = \sum \Delta \; of \; applicable \; exploitable \; factor$$

The ERE value can then be used to calculate the Return on Investment (ROI) for the TOI:

$$ROI \; equivilent = \frac{ERE}{Cost \; in \; millions}$$

Organizations are encouraged to prioritize investments with higher cost effectiveness. If there are investments with similar cost effectiveness, prioritize by impact. For those with similar cost effectiveness and impact, organizations should prioritize investment for applications of lowest cost.

Table 7. RAND Strengths and Weaknesses/Gaps.

Strengths	Weaknesses/Gaps
Approach includes both qualitative and quantitative information in its calculations	Process relies on subjective assessments for how investment reduces 'exploitability'
	Process does not consider threat environment
	Investments are focused on reducing 'exploitability' rather than other aspects (such as resiliency)
	Limited data to support evaluation of starting and implementation values for investment
	Cost is difficult to measure

Ability to Calculate CIE Value

The RAND methodology was designed to calculate the ROI of a proposed project and compare it to several other project proposals in a semi-quantitative way. Theoretically, this calculation could be modified to evaluate CIE value added.

A.2 Value Analysis or Value Engineering (VAVE)

Value Analysis (VA) (or Value Engineering (VE)) seeks to improve the value of a product, process, or service by analyzing its function relative to its cost. VA aims to validate that the function—defined as what the product, service, or system does for the user—is delivered at the lowest possible cost without compromising quality. This process involves carefully examining the existing design to identify areas where functionality can be enhanced or maintained while optimizing or reducing costs.

$$Value = \frac{Function}{Cost}$$

$where,$

$Function = the\ essential\ purpose\ or\ performance\ of\ the\ product\ or\ process$

$Cost = all\ expenses\ associated\ with\ delivering\ that\ function, including\ materials, labor, and\ overhead$

$Value = the\ value\ of\ the\ design$

VA encourages organizations to maximize this ratio, meaning either increasing functionality without proportionately increasing costs or maintaining functionality while reducing costs.

Table 8. VAVE Strengths and Weaknesses/Gaps.

Strengths	Weaknesses/Gaps
Straightforward and structured process with some quantitative value determination	Focused on modifications to new/existing products during the design phase
Process offers a secondary benefit in its ability to uncover system design flaws	Would need to be adapted to security improvement processes of CIE
	Many cybersecurity investments provide value beyond simple cash flow
	Measurement of loss, vulnerability, and effectiveness is difficult

Ability to Calculate CIE Value

VA's focus on critical functions aligns well with CIE's emphasis on understanding the key functions of a system or device; however, its lack of consideration to safety and reliability is a limiting factor.

A.3 Cyber Value-at-Risk (CVaR)

Cyber Value-at-Risk (CVaR) is a methodology "designed to take account of the potential harm that can arise from cyber-threats, and the variable effectiveness of commonly-used risk controls."[20] The origins of CVaR stem from the financial concept of value-at-risk (VaR), used to articulate a given bank's level of financial risk or the risk imposed by a specific investment portfolio.[21] Accurate CVaR's are important for both defenders and cyber insurers, who rely on

[20] Erola, Arnau, Ioannis Agrafiotis, Jason R.C. Nurse, Louise Axon, Michael Goldsmith, and Sadie Creese. "A System to Calculate Cyber Value-at-Risk," Vol. 113. Computers & Security, 2021.

[21] Buith, Jacques. "The Benefits, Limits of Cyber Value-at-Risk." *The Wall Street Journal*. Accessed August 7, 2024. https://deloitte.wsj.com/cio/the-benefits-limits-of-cyber-value-at-risk-1430712132.

CVaR data to underwrite policies and help organizations transfer cyber risk. Unfortunately, one of the primary weaknesses of this approach is that there is no consensus on what constitutes a good risk control. As noted by Erola et al., "…risk controls typically viewed as necessary by the professional and expert community are generally not underpinned by any framework that facilitates rigorous reasoning, quantification or qualification of the benefits resulting from their deployment."[22] This is the gap that CVaR attempts to fill by providing a method to calculate the likely "exposure to losses given the effect of deploying a specific risk control."[23] Put another way, CVaR is designed to measure the ***effectiveness*** of a given security control.

One of the main challenges with implementing a CVaR methodology is accurately calculating the likelihood or probability that an adverse event will occur. Many researchers have pursued Monte Carlo and probabilistic models to describe the frequency and likelihood of an event occurring, including the previously referenced Erola et al. This approach has its limitations; although sufficient data may exist with cyber insurers (related to the most commonly seen events), availability of this data is limited. This reality is compounded when considering outlier or Black Swan events, in which case the outcomes (or the attack methods) cannot be reasonably predicted.

A variety of complex models and formulas have been created for CvaR; however, a simplified interpretation from researchers at the National Renewable Energy Laboratory (NREL) is included here. The NREL "Cybersecurity Value-at-Risk" framework evaluates a given control and provides a "VaR score."[24]

$$VaR = L * (1 - CI) * I$$

$where,$

$L = likelihood\ of\ an\ attack\ or\ an\ event\ resulting\ in\ an\ impact$

$CI = control\ implementations\ weighted\ according\ to\ unmitigated\ risks$

$I = the\ impact\ score\ that\ is\ categorized\ as\ low, medium, or\ high$

A summary of identified strengths and weaknesses is included in **Table 1**.

APPLICATION OF CVAR (OR VARIANTS TO CIE)

The value of CVaR is best demonstrated with organizations considering (at least) two Courses of Action (CoA) to mitigate a particular risk or adverse event (i.e., "Should I choose option A or option B?"). Considered CoAs can include both solutions that align to CIE Principals and those that do not; however, this approach is limited to mitigating a specific, identified impact.

---

[22] Erola, Arnau, Ioannis Agrafiotis, Jason R.C. Nurse, Louise Axon, Michael Goldsmith, and Sadie Creese. "A System to Calculate Cyber Value-at-Risk," Vol. 113. Computers & Security, 2021.
[23] Erola, Arnau, Ioannis Agrafiotis, Jason R.C. Nurse, Louise Axon, Michael Goldsmith, and Sadie Creese. "A System to Calculate Cyber Value-at-Risk," Vol. 113. Computers & Security, 2021.
[24] Cryar, Ryan, and Anuj Sanghvi. "The Cybersecurity Value-at-Risk Framework." NREL, July 17, 2023. https://www.nrel.gov/docs/fy23osti/86899.pdf.

Table 9. Potential strengths and weaknesses of leveraging CVaR for business risk mitigation or other business justification calculations. (This list is not all-inclusive.)

Strengths	Weaknesses/Gaps
Relatively straightforward to apply for comparison of two potential controls	May overlook the risk associated with less frequent or unpredictable events
Considers the potential impact of an adverse event when considering security investments	Considers control efficacy on a scenario-by-scenario basis, and therefore may be difficult to apply if considering security programs or other investments that do not align to a specific attack scenario/adverse event of concern
	Does not (directly) consider the criticality of the systems affected by a scenario. (Initial impact (1st order effect) is evaluated; however, interdependencies for business operations may be overlooked.)
	Calculates "value" but does not consider cost or timelines for implementation, which may prohibit the selection of a specific option

A.4 Process Hazard Analysis (PHA) / Cyber PHA

The primary purpose of a Process Hazard Analysis (PHA) is to identify, evaluate, and control potential hazards associated with industrial processes. By systematically analyzing these hazards, organizations aim to ensure the safety of personnel, the environment, and the facility.

> *"Cyber PHA/Cyber HAZOP Cyber PHA, or cyber HAZOP, was one of the first methods developed by the general cybersecurity community (not specifically by process safety engineers) to assess risk associated with industrial control accidents caused by cyberattack."*[25]

At a high level, the PHA methodology includes five steps:

1. **Scenario Generation** – Organizations identify the initial event that could lead to a hazard and determine the potential consequences if no controls are in place.
2. **Evaluate Existing Controls** – Organizations list existing controls that can mitigate the hazard and assess how these controls affect the scenario.

[25] Marszal, Edward M. and Jim McGlone. *Security PHA Review for Consequence-Based Cybersecurity*. International Society of Automation (ISA) (2019): Research Triangle Park, NC.

3. **Assess Risk** – Organizations calculate the risk of the scenario using the following formula:

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

Afterwards, organizations prioritize scenarios based on their calculated risk and identify the scenarios that need further mitigation.
4. **Identify New Controls** – If any scenarios are identified that move beyond acceptable risk, the organization should propose new controls to mitigate identified risks and evaluate how the new controls will affect the scenario.
5. **Identify Security Levels** – For a Security PHA, there is an additional step. Each scenario is evaluated to determine if an adversary could defeat all countermeasures or bypass detection mechanisms. If yes, a Security Level (SL) for the adversary is assigned. This activity is repeated for all identified scenarios.

Table 10. PHA/ Cyber PHA Strengths and Weaknesses/Gaps.

Strengths	Weaknesses/Gaps
Scenarios are based on plausible failures.	PHA is a qualitative methodology.
	Often uses simplified system dependencies that may not fully represent the real-world complexities of the process.

Ability to Calculate CIE Value

PHA uses a qualitative methodology to evaluate mitigations by their impact on risk. There is no mechanism for quantifying the risk, impact, or value. Therefore, it would be necessary to supplement PHA with an additional decision-making tool, such as cost-benefit analysis, to calculate the value of CIE.

A.5 Layers of Protection Analysis (LOPA)

Approach

Layers of Protection Analysis (LOPA) typically uses orders of magnitude categories for initiating event frequency, consequence severity, and the likelihood of failure of independent protection layers to approximate the risk of a scenario. This is used to determine if there are sufficient layers of protection against an accident scenario (i.e., sufficient defense-in-depth to prevent the scenario from occurring).[26]

[26] *Layers of Protection Analysis*, Center for Chemical Process Safety (October 2001): New York, New York.

A summary of the LOPA methodology is as follows:

1. **Develop Scenario** – This includes identifying the hazardous event, defining the consequence and severity and estimating the initiating event frequency.
2. **Independent Protection Layers (IPLs) Assessment** - Identify the applicable IPLs that can prevent or mitigate the event or mitigate the event's impact and determine the Probability of Failure on Demand (PFD) for each IPL.
3. **Calculate the frequency for the event** - The mitigated event frequency is calculated by multiplying the frequency of the initiating event by the PFDs of all the IPLs in series. The equation is:

$$f_i^C = f_i^1 * \prod_{j=1}^{J} PFD_{ij}$$

4. **Assess event's frequency** - Compare calculation with the organization's risk appetite. If the results are outside the bounds, then develop additional measures and repeat steps 2 and 3 until the results are acceptable.

Table 11. LOPA Strengths and Weaknesses/Gaps.

Strengths	Weaknesses/Gaps
LOPA considers the impact due to the Independent Protection Layers (in this case the changes implemented due to CIE)	LOPA requires probability of failure, which in the context of CIE would be a cyber event and can be difficult to calculate.
	LOPA provides a snapshot of time. Over time adversary's capabilities grow, and this can impact the event frequency calculation.
	LOPA may not fully capture the complex interactions between different layers of protection and other system components or additional cybersecurity controls which could impact the event frequency calculation.
	LOPA is primarily a safety-focused tool and, as such, may not align with business objectives and strategic goals.

Ability to Calculate CIE Value

LOPA focuses on identifying and lowering the frequency of the scenario. However, the LOPA methodology is not designed to calculate the "value" or ROI of a given IPL. Because of this, integration or modification of the LOPA process to calculate a CIE value (e.g., reduction in

damages in the event of a cyber-attack), would likely need to include an additional step (such as cost/benefit analysis) to meet CIE's needs.

A.6 Infrastructure Susceptibility Analysis (ISA)

Infrastructure Susceptibility Analysis is a MITRE developed process designed to identify and assess adversary capability to target, manipulate, or hold a given CPS at risk.[27] The ISA methodology formalizes adversary assessments, enabling organizations to consistently track adversary capability growth, while minimizing analytic bias. The process extends traditional cyber threat intelligence approaches by considering sources of information typically overlooked by traditional cyber assessments (e.g., adversary offensive programmatic goals), and includes them in evaluations to identify the most likely technical targets of adversary cyber operations. This information is then used to prioritize cybersecurity investments for greatest impact.

Table 12. ISA Strengths and Weaknesses/Gaps.

Strengths	Weaknesses/Gaps
Analytic process enables prioritization of limited cybersecurity resources to areas of greatest risk (based on likelihood of adversary targeting and success)	Requires organizations to track and assess threat actor capabilities at regular intervals (i.e., trend analysis)
	Susceptibility calculations (and reduction in susceptibility) are considered on an individual attack scenario basis

Ability to Calculate CIE Value

ISA is designed to calculate the "susceptibility" of a given device or system to a specific cyber-attack and is similar to attack surface calculations. ISA susceptibility scores could be compared before and after implementation of a CIE-inspired solution. In this case, the value of CIE would be defined as a reduction in susceptibility for a given attack.

[27] "Infrastructure Susceptibility Analysis and Assessments | MITRE." Accessed September 17, 2024. https://www.mitre.org/news-insights/fact-sheet/infrastructure-susceptibility-analysis-and-assessments.

Cyber-Informed Engineering

INL/MIS-24-81663-Rev000