INL/MIS-23-75497-Revision-0

CRITICAL FUNCTION ASSURANCE: Understanding Critical Function and Critical Function Delivery is Foundational for Meaningful ICS Security Improvement and Policy Efforts

Jeffrey R Gellner, Curtis P St Michel, Sean McBride, Micah Rich Steffensen

Idaho National Laboratory

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-23-75497-Revision-0

CRITICAL FUNCTION ASSURANCE: Understanding Critical Function and Critical Function Delivery is Foundational for Meaningful ICS Security Improvement and Policy Efforts

Jeffrey R Gellner, Curtis P St Michel, Sean McBride, Micah Rich Steffensen

November 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

CRITICAL FUNCTION ASSURANCE

Understanding Critical Function and Critical Function Delivery is Foundational for Meaningful ICS Security Improvement and Policy Efforts

Jeffrey R. Gellner
Micah R. Steffensen
Curtis St. Michel
Sean Mcbride

Idaho National Laboratory

ABSTRACT

Modern life is enabled by a complex and interdependent web of critical functions, including energy, communications, transportation, food, and water. Automation has significantly reduced or replaced human interactions in the delivery of these functions, resulting in a web of goods and services that are made available 24/7 only through unique and intentional deployments of microprocessors, software, and firmware technologies. The prospect of cyber-enabled sabotage of these processes disrupts traditional risk determination models. Critical Function Assurance (CFA) is a foundational approach to identifying, prioritizing, and mitigating the risk that is inherent in the delivery of critical functions that depend on digital technology. It provides rapid focus to what matters most and illuminates elements and areas of risk that otherwise are often overlooked. This focus enables effective application of available security resources and optimizes security strategy and policy efforts. This paper introduces CFA to decision makers and risk executives (including CEOs, COOs, CFOs, and CISOs) whose organizations support and deliver the critical functions that underpin national defense, societal health and safety, and a vibrant economy.

CONTENTS

INTRODUCTION

Technology has fundamentally changed how we engineer and deliver every aspect of modern life, and these changes, coupled with international standardization, have catalyzed the growth of global supply chains, spurred financial exchange, and fostered the use of unique expertise from across the globe.

The reliable delivery of critical functions such as energy, communications, transportation, food, and water are foundational to growth and progress. Over the past 50 years, the potent combination of technological advancement and capital investment in these functions has allowed relatively small teams to support the needs of millions.

Modern power plants require fewer and fewer employees to maintain them. Control room operators for water provisioning systems can work from home. Farm implements are increasingly driverless.

As digital systems come under attack, with cyber-enabled sabotage as the primary aim, a paramount concern for the future is to assure the delivery of these critical functions, which are so dependent on and infused with digital technology.

When we are concerned, we use risk determination to inform “how” concerned we should be. Traditional risk management approaches build on risk pooling, where the consequences of occasional adverse events can be overcome by pooling a marginal amount of the gains obtained when adverse events do not occur. Under this theory, the “marginal amount” that owners and investors set aside is calculated from a predicted estimate of the intensity and frequency of adverse events. In other words, really bad things happen so infrequently, or the “likelihood” of X bad thing happening is so low, that we can often achieve significant risk mitigation with a minimum of operational change (primarily due to cost or increased effort).

Traditional risk determination assumes an ability to estimate the frequency and intensity of adverse events based on extensive historical record of failures, but the highly dynamic nature of the technological environments that deliver critical functions (as described above) may outpace our ability to accurately interpret or even capture the data representing some failure modes. **Furthermore, unlike other risk management paradigms, when considering cyber-enabled sabotage as the cause for a critical function disruption, determining the probability of such an event becomes nearly impossible, and at best highly speculative.**

We assert that when human behaviors and choices are the causal drivers of an event, that event can no longer be considered an “Act of God,” bad luck, or random chance. In these cases, we must move past probabilistic event categorization and focus on the highest impact events as a starting point for modern critical functional assurance.

Focusing on event impact instead of event probability has gained traction over the past 10 years, but **to truly determine which events have the highest impact on a critical function, teams must first understand critical function delivery.**

Critical function delivery has evolved dramatically, both in how functions are delivered and who manages them. Broad increases in automation and the ubiquitous use of digital technology now underpin nearly every aspect of enabling functions—those functions that answer "how" critical functions are delivered. Adding to the complexity and risk exposure is the realization that many functions traditionally performed in-house have been outsourced to a remote/global service and supply chain, into which there is far less visibility, and much less influence.

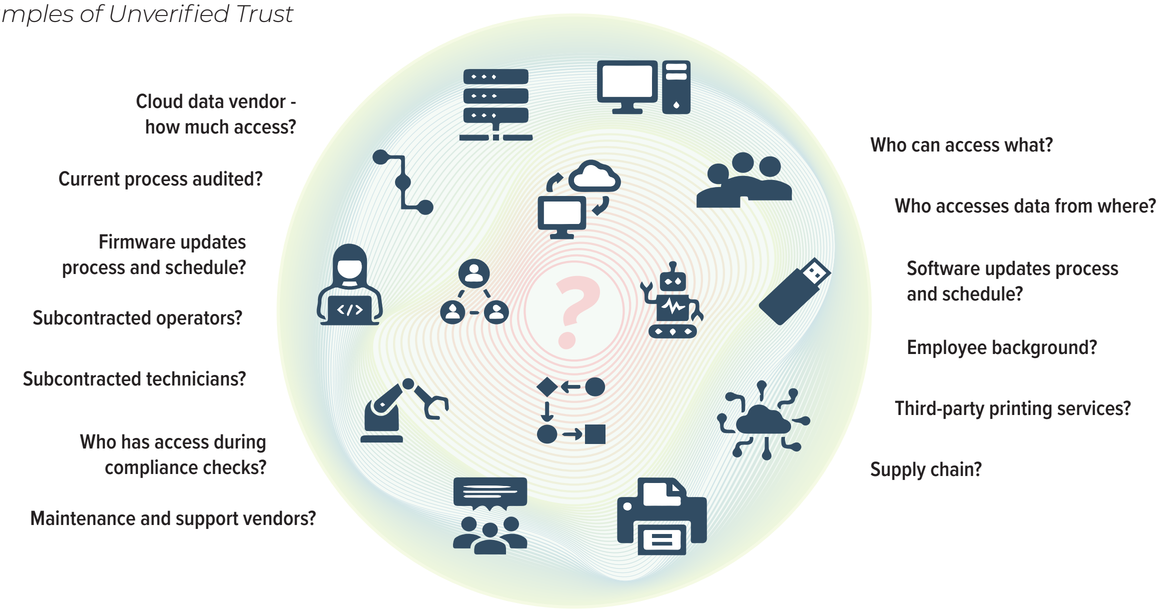
The dark side of technological development, deployment, and dependency—the seeds of destruction, and a missing link to most ICS/OT security approaches—is the reluctance and inability to fully understand and anticipate the consequences of how technologies are used in specific strategic functional delivery models. The complexity introduced by modern critical function delivery obscures the "unverified trust" that is being placed in people, systems, and processes (Figure 1).

Going forward, it is vitally important for organizations to understand how digital transformation has changed their risk exposure to potential cyber-enabled sabotage. Establishing and maintaining true resilience requires a fundamental shift in how we look at the cyber risk to critical function delivery.

In summation, CFA is an approach to prioritize and address risk based on impact and is rooted in a holistic understanding of how critical functions are delivered. It provides rapid focus to what matters most and illuminates elements and areas of risk that otherwise are often overlooked. This focus enables effective application of available security resources to the most vital areas of a business/mission/organization and provides the foundation for optimizing greater security strategy and policy efforts.

FOR OVER 20 YEARS, the Idaho National Laboratory (INL) has focused on Critical Function Assurance (CFA) and specifically the role that ICS/OT play in assuring critical functions and missions in the digital age. INL championed the concept of Cyber-informed Engineering (CIE) and created a robust and repeatable methodology to apply CIE principles through Consequence-driven Cyber-informed Engineering (CCE). Much of what is outlined in this paper comes from the years of experience gained exercising and vetting this approach.

Figure 1. *Examples of Unverified Trust*


Cloud data vendor - how much access?
Current process audited?
Firmware updates process and schedule?
Subcontracted operators?
Subcontracted technicians?
Who has access during compliance checks?
Maintenance and support vendors?
?
Who can access what?
Who accesses data from where?
Software updates process and schedule?
Employee background?
Third-party printing services?
Supply chain?

UNDERSTANDING CRITICAL FUNCTIONS AND CRITICAL FUNCTION DELIVERY

To “assure” means to make sure or certain. Hence, CFA is an approach for making sure the challenge of delivering critical functions is met. For many years now, the need to identify critical functions, prioritize them (increasingly based on consequence), and assure them has been well documented (e.g., DOD mission assurance, DHS Section 9), but implementation has been uneven.

Broadly speaking, a critical function can be defined as the actions or activities that make up the organization’s primary mission or purpose. An organization’s Critical Function, then, is what that organization does and why they exist (e.g., produce semiconductor wafers, move bulk volumes of natural gas or electrical power, or make medicine). Critical Functions are often referenced in an organization’s mission or vision statements.

The advantage of approaching functional risks in our organizations using CFA is the ability to understand logical and physical Critical Function delivery; we call this an organization’s Enabling Functions—the subset of people, process, technologies, information, and infrastructure (PPTII) that are essential for the delivery. Conversely, destruction, disruption, denial, or degradation of the Enabling Functions will impact the Critical Function (Figure 2).

This is an important and unique starting point for protecting our critical functions because it provides an immediate focus and prioritization of an organization’s efforts to protect what is most valuable to them. This contrasts with a traditional “security” approach of beginning with technology deployment, architectures, and choosing a security framework.

Critical and Enabling Functions

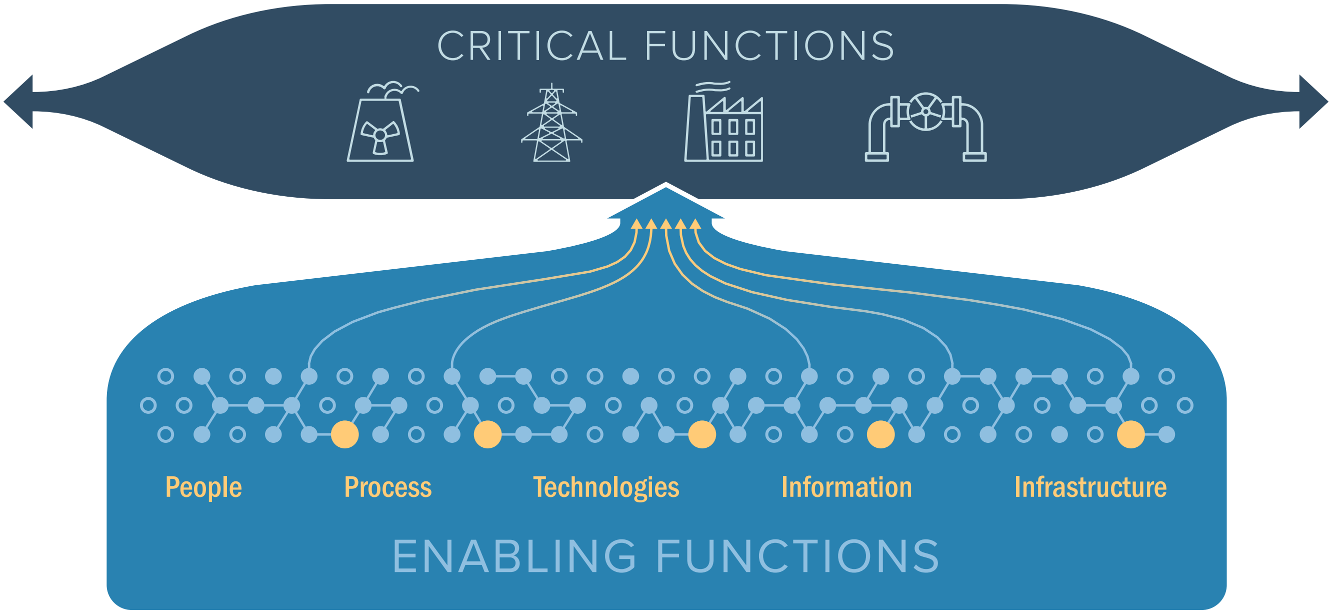


Figure 2. *Enabling Functions: People, Process, Technologies, Information, and Infrastructure the organization uses to both logically and physically deliver Critical Functions*

CFA moves the practitioner beyond narrow considerations of discrete technological deployments by including the operational and engineering context required to describe critical function delivery holistically and accurately. Understand, the CFA approach is not meant to *replace* existing cybersecurity practices, but rather to *introduce focus* on what is most critical to the organization, thereby enhancing these practices and all other security efforts (Figure 3).

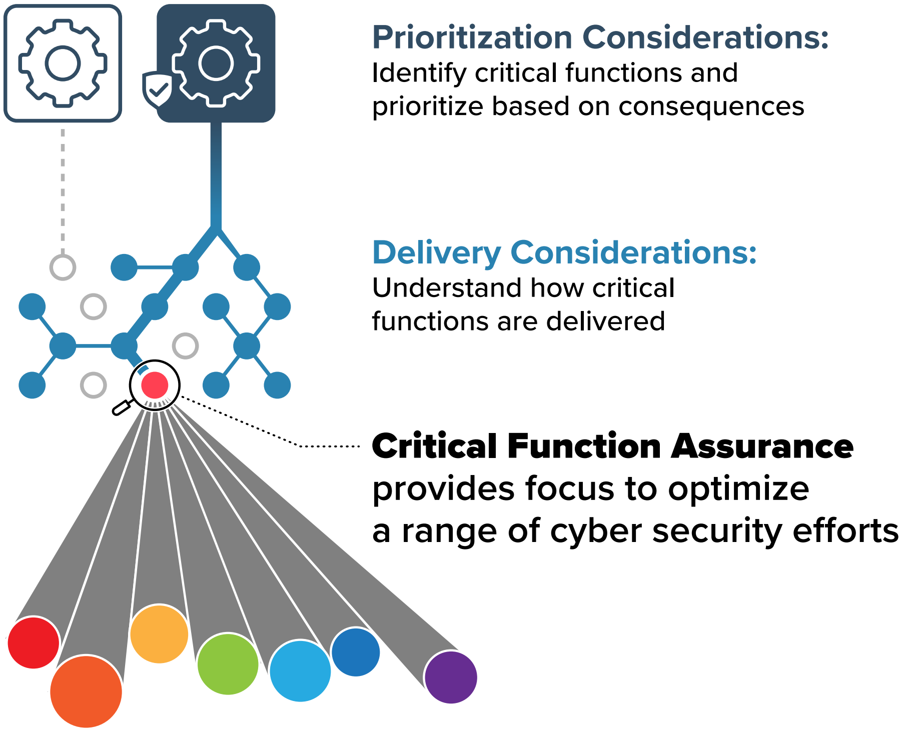

Prioritization Considerations:
Identify critical functions and
prioritize based on consequences
Delivery Considerations:
Understand how critical
functions are delivered
Critical Function Assurance
provides focus to optimize
a range of cyber security efforts

Figure 3. *Critical Function Assurance (Digital Dependence)*

It is also worth noting that like traditional assurance or risk management strategies, CFA has several components. For example, in the delivery of any given Critical Function, there will be considerations for the financial assurance, physical assurance, and digital assurance of the function itself. The purpose of the remainder of this paper will be to focus on how to better understand risk exposure in functional delivery from the digital dependence perspective and how to apply steps that can help focus industrial control system (ICS)/ operational technology (OT) security to better assure critical functions.

This paper advances Critical Function Assurance as a guiding approach to address these concerns. As approaches represent a foundational way to view the problem, it is worth noting that much of our experience practicing and achieving functional assurance has come from following the Consequence-driven Cyber-informed Engineering (CCE) process. The four-phase CCE process can be effectively applied to any functional delivery paradigm and was developed specifically to accomplish the goals of CFA. This paper will not outline specific steps or processes, but instead intends to simply describe the key principles and benefits of the CFA approach.[1]

[1] For more information on the CCE process, see https://inl.gov/cce/.

CFA IN PRACTICE

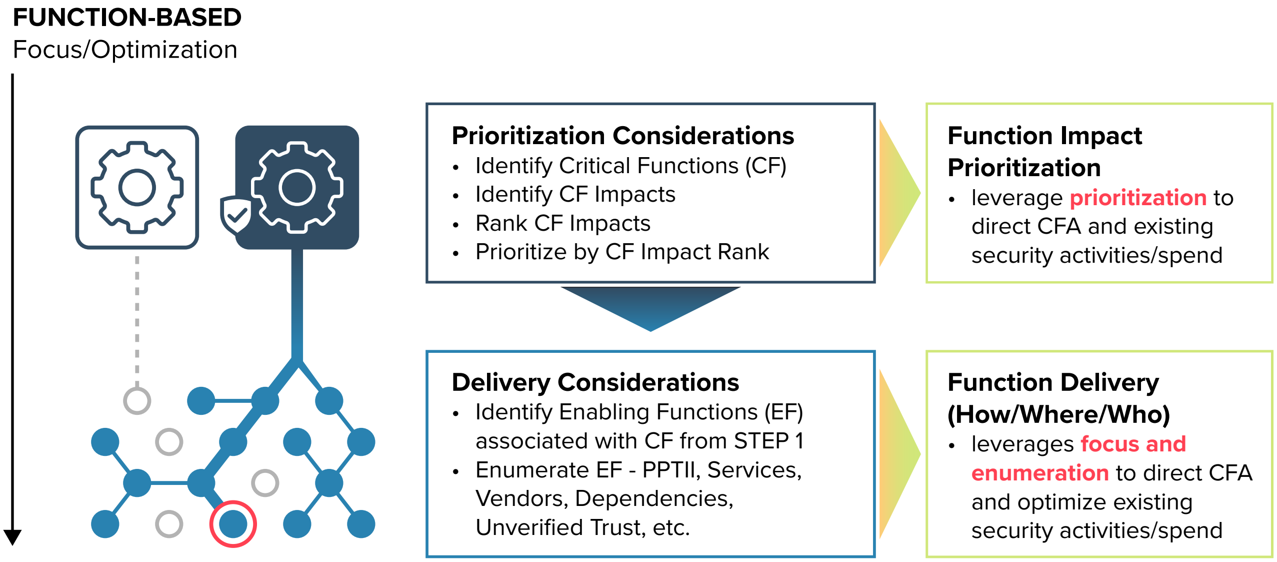
CRITICAL FUNCTION IMPACTS — PRIORITIZATION AND FOCUS

Few would disagree with the notion that an organization's security efforts should primarily support and protect achieving business objectives. This core idea is what we call Critical Function Assurance. Organizations traditionally allocate human and capital resources to security efforts precisely to achieve that level of protection; however, traditional approaches can result in a scattershot security strategy.

The challenge is the mental model of what teams "have" in their organizations. Teams tend to look at their organizations, their production systems, or any digitally enhanced environment, as an inventory list of assets defined by technological makeup (hardware x, OS y, applications z). Security and risk mitigation activities are then largely identified and prioritized based on those inventories and the assets' perceived value. For example, the following platforms are common and provide immense business value to many organizations, but may not be the most important element for security considerations by measure of critical function delivery and impact: ERP, GRC, HR, MES, QMS, EPP, EDR, EMS, or SCADA, etc.

Our position is that the traditional approach is not wholly incorrect, but it is incomplete and ultimately inadequate (akin to "flock shooting") without functional consideration and prioritized application.

We propose instead to begin by asking a few questions: *What are the organization's Critical Functions? How does it deliver them through Enabling Functions? How does the risk exposure of the Enabling Functions translate to business impact risk?* The CFA approach (Figure 4) provides a way to address these questions.



Prioritization Considerations
- Identify Critical Functions (CF)
- Identify CF Impacts
- Rank CF Impacts
- Prioritize by CF Impact Rank

Function Impact Prioritization
- leverage **prioritization** to direct CFA and existing security activities/spend

Delivery Considerations
- Identify Enabling Functions (EF) associated with CF from STEP 1
- Enumerate EF - PPTII, Services, Vendors, Dependencies, Unverified Trust, etc.

Function Delivery (How/Where/Who)
- leverages **focus and enumeration** to direct CFA and optimize existing security activities/spend

Figure 4. *CFA Prioritization and Delivery Considerations*

To develop an optimization of our security activities and work deliberately toward CFA, teams need to first understand how their organization's Critical Functions are delivered. They need to enumerate the Enabling Functions (e.g., PPTII, analytics, data flow, ancillary dependencies — power/water/air/raw materials, etc.) that directly support delivery. Doing so provides an immediate focus and prioritization of security efforts to a subset of the greater business environment.

CRITICAL FUNCTION DELIVERY — IDENTIFY AND UNDERSTAND

ENABLING FUNCTIONS: *The people, process, technologies, information, and infrastructure (PPTII) the organization uses to both logically and physically deliver Critical Functions.* It is worth noting that Enabling Functions are not separate from, or in addition to, the myriad of PPTII supported in traditional security efforts throughout an organization—they are embedded, a subset, and inextricably linked.

Consider the case of a discrete manufacturing process; each stage of the process is required to achieve a desired manufactured product. In terms of potential impact to the organization's ability to manufacture the product, **a single stage of the process may be deemed most important.** Like the other stages, this single stage of the process occurs by leveraging a specific aggregation of people, processes, technologies, information, and infrastructure. It may be helpful to think of the stage broken down by assessing what elements of PPTII are being used and how.

> **For instance, the stage is accomplished:**
>
> - *on this* **digital equipment**…
> - *using this* **software/hardware/firmware**…
> - *at these* **network locations**…
> - *by these* **people**…
> - *with support from these* **vendors**…

These PPTII are finite and can be understood and prioritized for security efforts. We can build resilience through engineered protections and robust detection/response capabilities. We can know what to detect/monitor on our endpoints, our network traffic, where/how to improve access control, physical protection, and where to apply security best practices. With an engineering and operations-level understanding of relationships and functional dependencies in our production environments, our traditional security activities can be optimized.

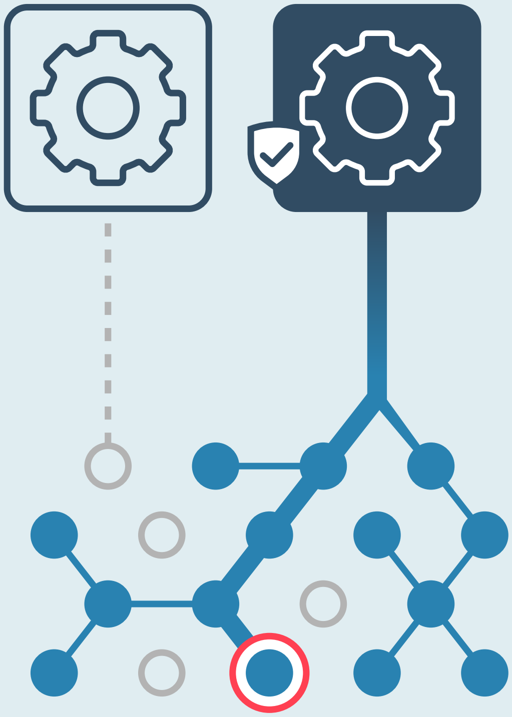
Understanding functional delivery in this way can be most effectively tackled by the teams that design, operate, and maintain that manufacturing stage—process engineers/technicians, automation engineers/technicians, production system operators, communications engineers/technicians, information system administrators, security administrators, etc. The following examples will illustrate how identifying Enabling Functions is key to understanding risk to an organization's ability to deliver their Critical Function.

APPLIED EXAMPLES: ENABLING FUNCTION ENUMERATION FOR CFA

The examples below consider variations of industrial-scale operation where there is extensive deployment and reliance on digital systems for situational and state awareness, decision making, control, and monitoring; and where global supply chains provide everything from digital and physical components to raw materials and assemblies to contracted services. These complex environments are best understood in the same way they are designed, engineered, commissioned, and operated—functionally. **Understanding function is a key to understanding risk exposure to delivery impacts.**

Physical damage in production assets is always a concern and should be a priority for minimizing risk exposure; however, the impact of physical damage to particular element(s) in a production system depends on the functional significance of those elements in the process. For some production systems, other concerns eclipse component physical damage in terms of overall delivery impact risk because recovery from damage to these elements is manageable.

Real-world, industrial-scale production systems almost certainly need CFA-focused security activities across a breadth of functions identified individually. **The following examples maintain a high-level perspective in describing delivery complexities in order to convey the key concepts in the CFA approach.**



PRIORITIZATION CONSIDERATIONS

Through identification and ranking of possible Critical Function impacts, the production (technical, operations, and business) SMEs determine that dependence on a specific subset of Enabling Functions presents the greatest risk exposure for the organization. Due to the operating context for the organization, the SMEs determine that the risk exposure here equals or exceeds all others.

DELIVERY CONSIDERATIONS

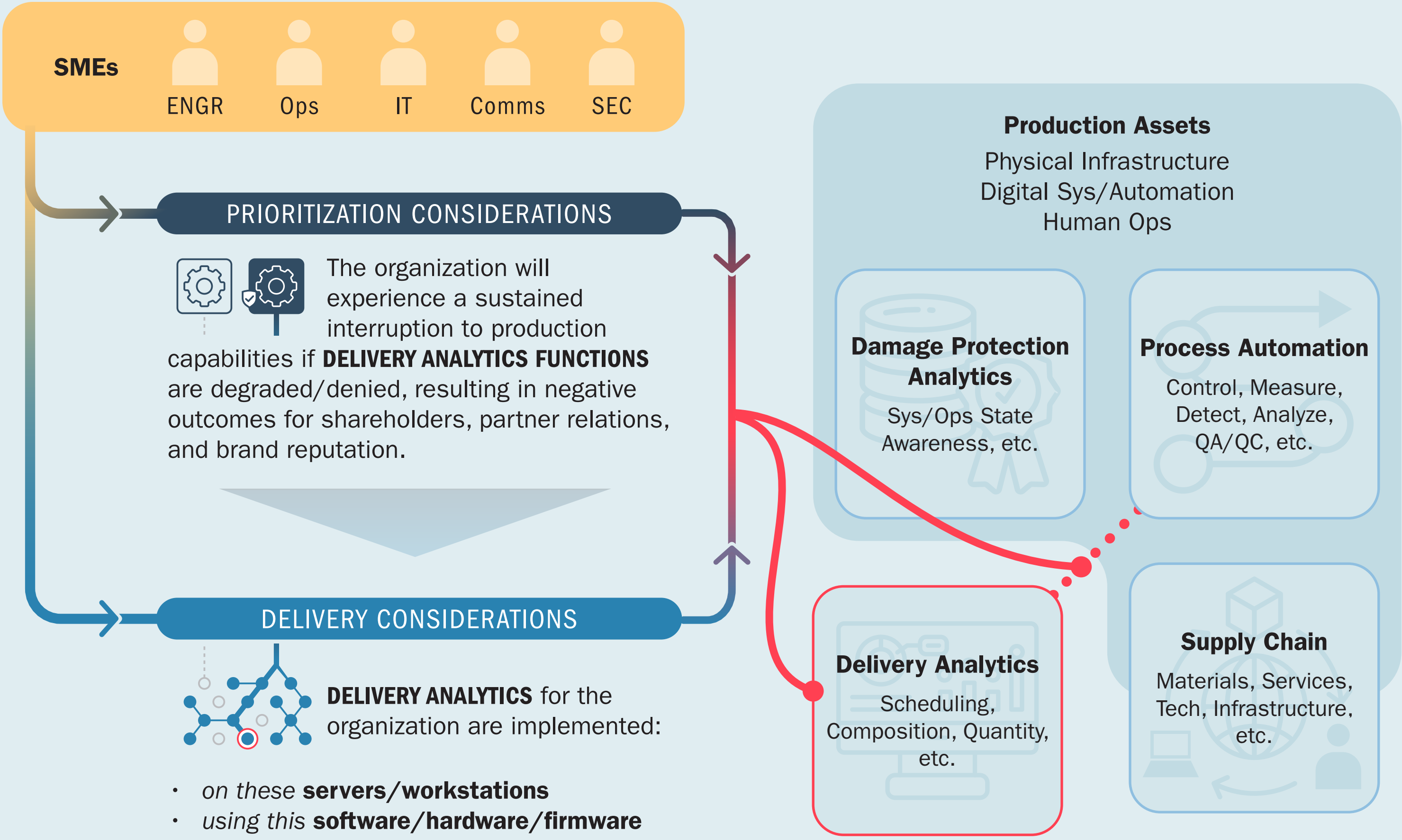
Through enumeration of the specific subset of Enabling Functions identified during Prioritization, the team of SMEs has determined that implementation warrants prioritized and expanded considerations for resilience improvements to involve security, communications, IT, and operations support.

For each example, ask: How would this ability to identify, prioritize, and understand a narrow band of critical function delivery focus/enhance the organization's security efforts?

EXAMPLE #1

DELIVERY ANALYTICS

Consider an organization where **DELIVERY ANALYTICS** drive asset use and determine success. This could be a liquid or gas product pipeline, a collection of distributed manufacturing facilities, or power delivery. Scheduling, market participation, product delivery and receipt verification, and production system operations are all dependent on the aggregation and analysis of specific data sets.



SMEs

ENGR Ops IT Comms SEC

PRIORITIZATION CONSIDERATIONS

The organization will experience a sustained interruption to production capabilities if **DELIVERY ANALYTICS FUNCTIONS** are degraded/denied, resulting in negative outcomes for shareholders, partner relations, and brand reputation.

DELIVERY CONSIDERATIONS

DELIVERY ANALYTICS for the organization are implemented:

- *on these* **servers/workstations**
- *using this* **software/hardware/firmware**
- *at these* **network locations**
- *by these* **people**
- *with support from these* **vendors...**

Production Assets
Physical Infrastructure
Digital Sys/Automation
Human Ops

Damage Protection Analytics
Sys/Ops State Awareness, etc.

Process Automation
Control, Measure, Detect, Analyze, QA/QC, etc.

Delivery Analytics
Scheduling, Composition, Quantity, etc.

Supply Chain
Materials, Services, Tech, Infrastructure, etc.

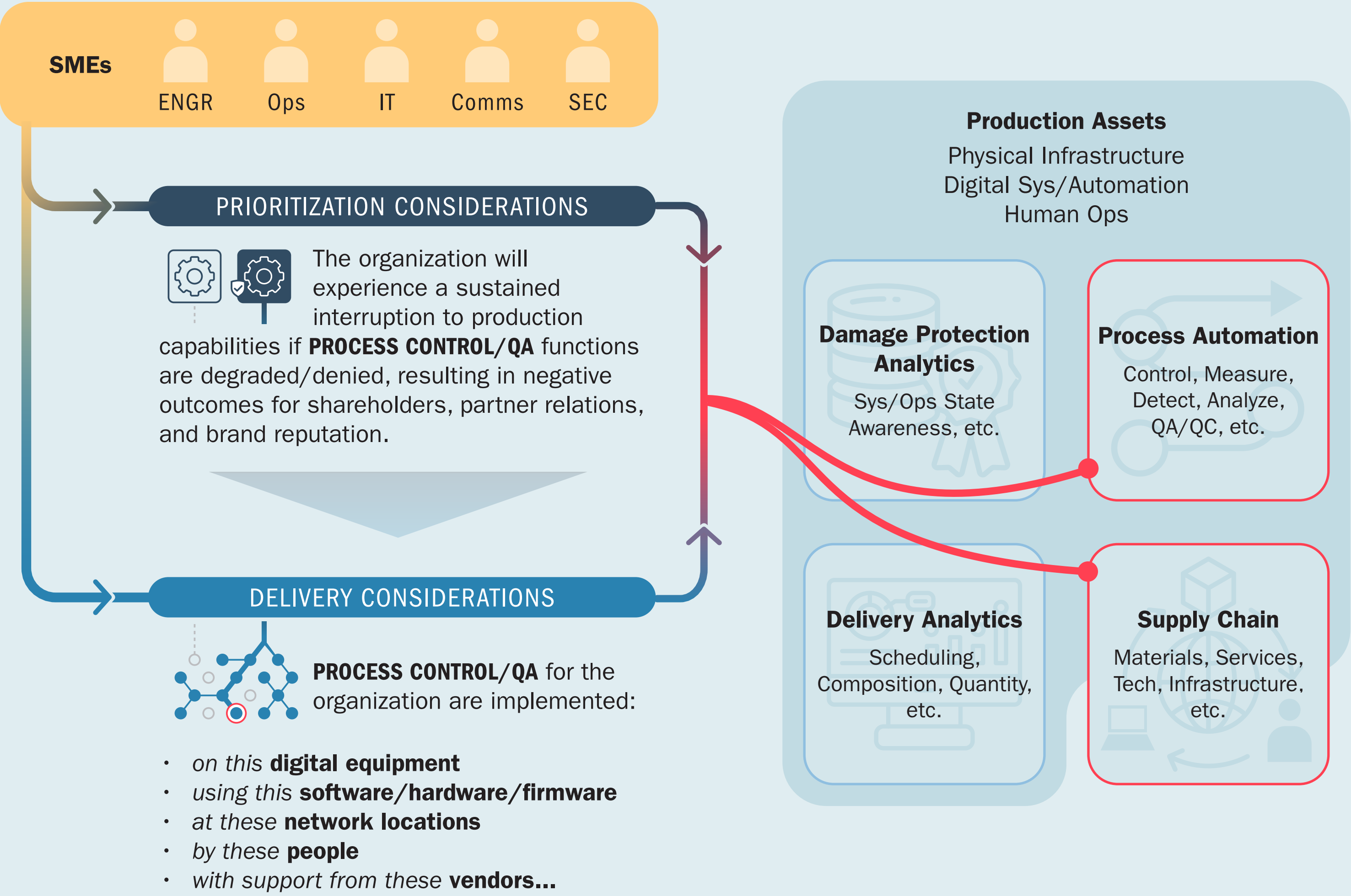
EXTENDED DELIVERY AND SECURITY CONSIDERATIONS

- What subset of traditional security activities would be especially useful based on the outcomes of CFA Prioritization and Delivery Considerations?
- For the implementation of **DELIVERY ANALYTICS**, what type of follow-on questions would inform our security activities? ***How is it accomplished (software, object/code, hardware, human)?* • *What are data/workflow dependencies?* • *What information is required for success/accuracy?* • *How is the information obtained?* • *Where does the information originate?* • *How is the information validated?* • *How are the analytics and dataflow architected?* • *Who supports? Internal/External?* • *What can we target for monitoring/alerting/response?* • *How can we confidently restore the delivery analytics functions?* • *Etc.***
- How does this compare to a generic, broad application of traditional security activities in terms of focus and empowerment to prevent or mitigate what functionally presents the greatest risk exposure to the organization?

EXAMPLE #2

PROCESS AUTOMATION

Consider an organization where **PROCESS AUTOMATION** determines success. The finished product quality and exacting composition is fundamental to the Critical Function and is a prerequisite for delivery execution. This could be petrochemicals, pharmaceuticals, food production, or other goods.



SMEs

PRIORITIZATION CONSIDERATIONS

The organization will experience a sustained interruption to production capabilities if **PROCESS CONTROL/QA** functions are degraded/denied, resulting in negative outcomes for shareholders, partner relations, and brand reputation.

DELIVERY CONSIDERATIONS

PROCESS CONTROL/QA for the organization are implemented:

- *on this* **digital equipment**
- *using this* **software/hardware/firmware**
- *at these* **network locations**
- *by these* **people**
- *with support from these* **vendors...**

Production Assets

Physical Infrastructure
Digital Sys/Automation
Human Ops

Damage Protection Analytics

Sys/Ops State Awareness, etc.

Process Automation

Control, Measure, Detect, Analyze, QA/QC, etc.

Delivery Analytics

Scheduling, Composition, Quantity, etc.

Supply Chain

Materials, Services, Tech, Infrastructure, etc.

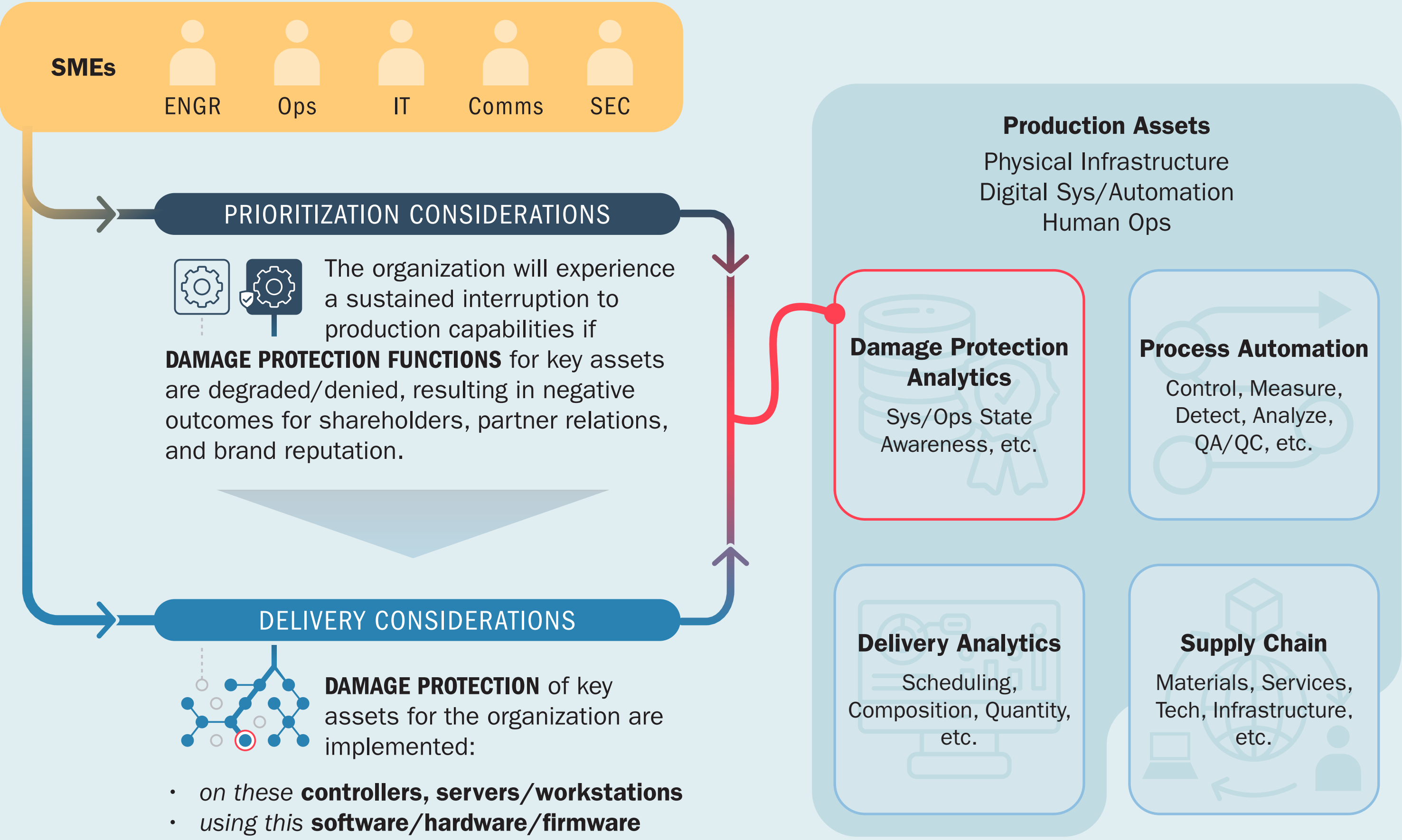
EXTENDED DELIVERY AND SECURITY CONSIDERATIONS

- What subset of traditional security activities would be especially useful based on the outcomes of CFA Prioritization and Delivery Considerations?
- For the implementation of **PROCESS CONTROL/QA**, what type of follow-on questions would inform our security activities? ***What process or subprocess are we controlling?*** • ***What process parameters are involved?*** • ***How are they measured?*** • ***How are they validated?*** • ***What production parameters are we inspecting for QA?*** • ***How are they accomplished (software, object/code, hardware, human)?*** • ***What is our supply chain support/dependency for the platforms?*** • ***Who supports internally?*** • ***What can we target for monitoring/alerting/response?*** • ***How can we confidently restore the process control/QA functions?*** • ***Etc.***
- How does this compare to broad application of traditional security activities in terms of focus and empowerment to prevent or mitigate what functionally presents the greatest rick exposure to the organization?

EXAMPLE #3

ASSET DAMAGE PROTECTION

Consider an organization where functionality and availability of key production system assets determine success. This could be a liquids/gas pipeline, a manufacturing facility, an aggregation/distribution facility, or power delivery. **DAMAGE PROTECTION** analytics, the sensing and protective action decision-making, may reside in a dedicated stand-alone platform or as part of a larger process automation system or both.



SMEs

ENGR Ops IT Comms SEC

PRIORITIZATION CONSIDERATIONS

The organization will experience a sustained interruption to production capabilities if **DAMAGE PROTECTION FUNCTIONS** for key assets are degraded/denied, resulting in negative outcomes for shareholders, partner relations, and brand reputation.

DELIVERY CONSIDERATIONS

DAMAGE PROTECTION of key assets for the organization are implemented:

- *on these* **controllers, servers/workstations**
- *using this* **software/hardware/firmware**
- *at these* **network locations**
- *by these* **people**
- *with support from these* **vendors...**

Production Assets

Physical Infrastructure
Digital Sys/Automation
Human Ops

Damage Protection Analytics
Sys/Ops State Awareness, etc.

Process Automation
Control, Measure, Detect, Analyze, QA/QC, etc.

Delivery Analytics
Scheduling, Composition, Quantity, etc.

Supply Chain
Materials, Services, Tech, Infrastructure, etc.

EXTENDED DELIVERY AND SECURITY CONSIDERATIONS

- What subset of traditional security activities would be especially useful based on the outcomes of CFA Prioritization and Delivery Considerations?
- For the implementation of **DAMAGE PROTECTION**, what type of follow-on questions would inform our security activities? ***What part of the process are we protecting?* • *Is our damage protection implemented within the process control platforms or separately as a dedicated platform or both?* • *What process parameters are involved?* • *How are they measured?* • *How are they validated?* • *Is damage protection implemented exclusively in digital form?* • *How is it accomplished (software, object/code, hardware)?* • *What is our supply chain support/dependency for the platforms?* • *Who supports internally? What can we target for monitoring/alerting/response?* • *How can we confidently restore the process control/QA functions?* • *Etc.***
- How does this compare to broad application of traditional security activities in terms of focus and empowerment to prevent or mitigate what functionally presents the greatest risk exposure to the organization?

CONCLUSION: CFA OPTIMIZES SECURITY ACTIVITIES TO ASSURE CRITICAL FUNCTIONS

Critical Function Assurance is an approach to prioritize and address risk based on impact and is rooted in a holistic understanding of how critical functions are delivered. It provides rapid focus to what matters most and illuminates elements and areas of risk that otherwise are often overlooked. This focus enables effective application of scarce security resources to the most vital areas of a business/mission/organization and provides the foundation for optimizing greater security strategy and policy efforts (Figure 5). It provides the analytic basis and focus to answer questions such as:

> *What in our business is most important to protect from cyber-enabled sabotage?* • *Where should we focus our general security efforts/resources?* • *Where should we engage in cyber-informed engineering efforts of devices or engineered solutions?* • *Where should we pen test, and what are we looking for?* • *Where should we conduct tailored monitoring and detection activities?* • *Etc.*

CFA is about protecting the reason for which a business/mission/organization exists, and it is foundational for meaningful ICS security improvement and policy efforts.

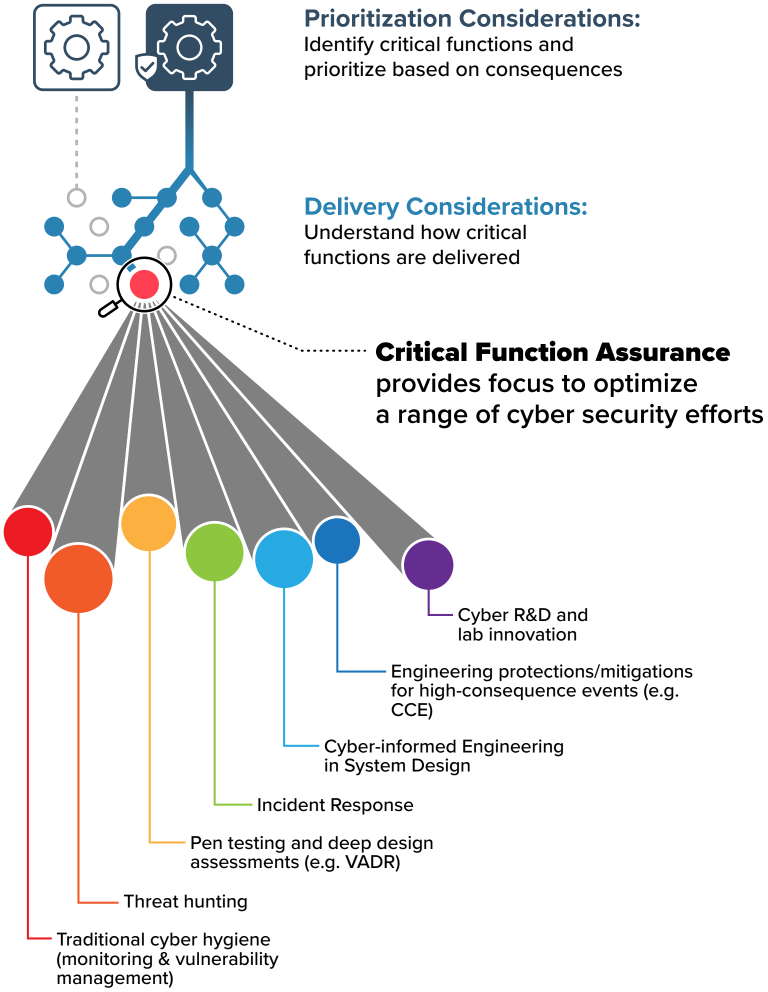

Prioritization Considerations:
Identify critical functions and prioritize based on consequences
Delivery Considerations:
Understand how critical functions are delivered
Critical Function Assurance provides focus to optimize a range of cyber security efforts
Cyber R&D and lab innovation
Engineering protections/mitigations for high-consequence events (e.g. CCE)
Cyber-informed Engineering in System Design
Incident Response
Pen testing and deep design assessments (e.g. VADR)
Threat hunting
Traditional cyber hygiene (monitoring & vulnerability management)

Figure 5. *CFA-Focus and Optimization of Security Efforts*

REFERENCES

Freeman, Sarah G., Curtis St Michel, Robert Smith, and Michael Assante. *Consequence-driven cyber-informed engineering (CCE)*. U.S. Department of Energy and Idaho National Laboratory, October 2016. https://doi.org/10.2172/1341416.

For more information about CCE, see: https://inl.gov/cce/.

Wright, Virginia L., Jakob P. Meng, Robert S. Anderson, Jeffrey R. Gellner et al. *Cyber-Informed Engineering Implementation Guide.* U.S. Department of Energy and Idaho National Laboratory, August 2023. https://www.osti.gov/biblio/1995796.

For more information about CIE, see: https://inl.gov/cie/.

U.S. Department of Defense. *Mission Assurance Strategy*. April 2012. https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. “National Critical Functions.” April 2019. https://www.cisa.gov/national-critical-functions.