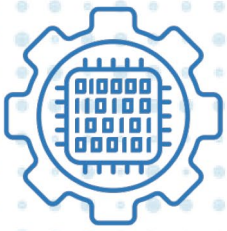


Cyber-Informed Engineering

Cyber-Informed Engineering Notes Workbook

CIE GDO GRIP Training

August 20, 2024

Authors:

Virginia Wright
CIE Program Manager

Benjamin Lampe
CIE Researcher

Contents

1. Workbook Purpose 4

2. Cyber-Informed Engineering Summary 4

2.1. PRINCIPLE 1: Consequence-Focused Design 6

2.2. PRINCIPLE 2: Engineered Controls 8

2.3. PRINCIPLE 3: Secure Information Architecture 10

2.4. PRINCIPLE 4: Design Simplification 12

2.5. PRINCIPLE 5: Layered Defenses 14

2.6. PRINCIPLE 6: Active Defense 16

2.7. PRINCIPLE 7: Interdependency Evaluation 18

2.8. PRINCIPLE 8: Digital Asset Awareness 20

2.9. PRINCIPLE 9: Cyber-Secure Supply Chain Controls 22

2.10. PRINCIPLE 10: Planned Resilience 24

2.11. PRINCIPLE 11: Engineering Information Control 26

2.12. PRINCIPLE 12: Organizational Culture 28

Acronyms

CIE	Cyber-Informed Engineering
INL	Idaho National Laboratory
IT	Information Technology
OT	Operational Technology

References

1. U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response*. Cyber-Informed Engineering Implementation Guide*. Version 1.0, August 7, 2023. https://www.osti.gov/biblio/1995796.

Figures

Figure 1 - CIE Principles and Key Questions.....5

1. Workbook Purpose

This workbook provides a notebook to capture insights and lessons learned provided by the discussion and application of the principles for Cyber-Informed Engineering throughout the workshop.

2. Cyber-Informed Engineering Summary

Cyber-Informed Engineering (CIE)[1] offers an opportunity to "engineer out" some cyber risk across the entire system lifecycle, starting from the earliest possible phases of conceptual design and requirements development and system design—the most optimal times to introduce mitigations against cyber risk. CIE is an emerging method to integrate cybersecurity risk considerations into the conception, design, development, and operation of any physical system that has digital connectivity, monitoring, or control. CIE uses design decisions and engineering controls to mitigate or even eliminate avenues for cyber-enabled attacks or reduce the consequences when an attack occurs.

In the same way that engineers design systems for safety, engineers informed by CIE use similar methods to prevent or lessen the impact of a cyber-attack. CIE also allows the engineers to advise the approaches used by specialized Information Technology (IT) and Operational Technology (OT) cybersecurity experts to align cybersecurity mitigations to the most critical consequences identified by the engineers. Working together, both parties actively implement engineered and cybersecurity solutions to address the highest-risk consequences in their systems, ensuring robust protection for their devices and infrastructure.

This workshop summarizes the principles for Cyber-Informed Engineering, provided with the principle's initiating question in Figure 1.

[1] U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. *Cyber-Informed Engineering Implementation Guide*. Version 1.0, August 7, 2023. https://www.osti.gov/biblio/1995796.

	PRINCIPLE	KEY QUESTION
1	**Consequence-Focused Design**	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
2	**Engineered Controls**	How do I select and implement controls to reduce avenues for attack or the damage that could result?
3	**Secure Information Architecture**	How do I prevent undesired manipulation of important data?
4	**Design Simplification**	How do I determine what features of my system are not absolutely necessary to achieve the critical functions?
5	**Layered Defenses**	How do I create the best compilation of system defenses?
6	**Active Defense**	How do I proactively prepare to defend my system from any threat?
7	**Interdependency Evaluation**	How do I understand where my system can impact others or be impacted by others?
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?
9	**Cyber-Secure Supply Chain Controls**	How do I ensure my providers deliver the security the system needs?
10	**Planned Resilience**	How do I turn “what ifs” into “even ifs”?
11	**Engineering Information Control**	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
12	**Organizational Culture**	How do I ensure that everyone’s behavior and decisions align with our security goals?

Figure 1 - CIE Principles and Key Questions

2.1. PRINCIPLE 1: Consequence-Focused Design

KEY QUESTION

How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?

PRINCIPLE OVERVIEW

Consequence-focused design is the first principle considered within a Cyber-Informed Engineering project. It results in insights that feed the remainder of the principles. **Consequence-focused design** begins with an analysis of the business purpose and its primary mission, the critical functions of the business, the interconnection of those functions to the system under consideration, and finally, the critical functions of the system itself. The team identifies the most consequential impacts, sometimes referred to as the high-consequence events (HCEs), that could result from disruption of the critical functions, especially those where the disruption of a system function could result in a mission-impacting consequence. The team develops a list of HCE's and prioritizes the most impactful. In the initial review, the team need not evaluate the potential or likelihood of these impacts being induced via digital failure or cyber-attack. Once HCE's are identified, the team can begin to explore how those effects could be realized via adversary attack or digital failure.

QUESTIONS

What are the systems that perform and support critical facility functions?

What are the unacceptable high consequence events that impact mission delivery, safety, security, the environment, equipment and property, financials, or corporate reputation?

What are the critical processes, operations, and/or administrative actions required to protect against unacceptable high consequence events?

How are identified high consequence events documented, monitored for change, and reassessed?

Which stakeholders (e.g. operations staff, engineering staff, executive leadership, external parties) would be impacted during or by damage from high consequence events and how are they included in mitigation decisions?

PRINCIPLE NOTES

2.2. PRINCIPLE 2: Engineered Controls

KEY QUESTION

How do I select and implement controls to reduce avenues for attack or the damage that could result?

PRINCIPLE OVERVIEW

For the most critical consequences and impacts determined in **Consequence-focused design**, we have an opportunity to think about the specific controls we'd like to have in place to prevent them. Eventually, we'll talk about the collection in terms of **Layered Defenses**, but at first, we can:

- Think about what kinds of controls we can have in place to prevent a consequence or mitigate its impact.
- Determine which controls are provided as a part of products and services we are using and which ones we might want to design in.
- Determine whether we can identify both physical controls and digital controls for a given consequence and the relative costs and benefits of each.
- Determine whether our controls prevent an attack, lower the impact of the attack, or serve to provide alarms or warnings of adverse situations.

QUESTIONS

How are the storage, movement, and use of hazardous quantities of mass or energy (potential and kinetic) controlled by digital technologies?

How are engineered systems (e.g., IT, operational technology [OT], electrical, mechanical pneumatic, mechanical hydraulic, thermal, chemical) that store, move and use hazardous quantities of product or energy dependent on digital technologies to support critical functions?

What consequences of failure or maloperation are the engineered controls designed to prevent?

Where engineered controls depend on digital technologies, where might an analog engineered control add to the protection (or lower the impact) of a high consequence event?

How do we monitor and ensure the effectiveness of engineering controls through system changes (e.g. expansion) and operational conditions, including those that may weaken their effectiveness (e.g. through undue stress)?

How do we validate the efficacy of engineered controls, especially those that may be affected or circumvented by administrative workarounds?

PRINCIPLE NOTES

2.3. PRINCIPLE 3: Secure Information Architecture

KEY QUESTION

How do I prevent undesired manipulation of important data?

PRINCIPLE OVERVIEW

Each system contains data linked to mission-critical consequences and impacts which should be protected from outsider view and, more importantly, adversary or failure-induced alteration. For each identified data element or stream, a **Secure Information Architecture** can be designed, guided by the consequences and impacts identified earlier, to segregate the most important data and the systems which contain it to provide more control, protection, and monitoring of those systems and that data.

We can start early in system design to identify those data elements most tied to a potential critical consequence, where they originate and are altered through the process, how they should be protected, and whether it is possible to design a data verification mechanism using the process, analog controls, or historic inputs.

Once our design is mature and the underlying network and data service architecture is under design, more fine-grained digital controls, and create specific zones and segmentation plans can be created.

QUESTIONS

What are the key data elements, the critical inputs and outputs, and the mechanisms (people, tools, systems) each process step that the system executes?

How independent are the key data elements, physically or digitally, to allow diagnosis of the extent or cause of an anomaly?

Which information exchanges with the system would result in a high consequence event if the data was disrupted or manipulated?

What engineering and operations-based protection and verification could ensure that key data elements have not been manipulated?

How could unanticipated adverse or extraordinary operating modes potentially violate security controls or validation mechanisms placed on the data?

PRINCIPLE NOTES

2.4. PRINCIPLE 4: Design Simplification

KEY QUESTION

How do I determine what features of my system are not absolutely necessary to achieve the critical functions?

PRINCIPLE OVERVIEW

Systems formed through acquisition often have more features than are explicitly needed to perform required functions. Though these features can be configured not to be available to authorized system users, they are available to adversaries who gain access. These features can potentially lead to catastrophic impacts if used by malicious adversaries.

In **Design Simplification**, we consider which features of the system are not absolutely necessary and of those, which could lead to impactful adverse consequences if misused. We consider how to reduce the system to the minimum elements needed to provide mission-critical functions and necessary resilience. For each of the non-essential features, we consider whether we can completely remove them. When that is not possible, we collaborate with cybersecurity specialists to determine how to implement alarms and alerts when those functions are leveraged, or whether we can capture undesired commands at a network segmentation boundary before they are executed.

QUESTIONS

Where are opportunities to simplify or eliminate device/system elements or features that are not necessary to meet the minimum functional capabilities and defined system requirements?

How would a given design simplification introduce tradeoffs (e.g., loss of redundant control, reduced reliability, reduced operator visibility) that conflict with other stakeholder requirements or downstream dependencies?

How do each of the design elements traceable to a specific project requirement or critical operation/process?

What non-digital alternative to a digital feature could be applied to satisfy a requirement?

Which system features used for supporting the operation and maintenance of the system by personnel not necessary (e.g., engineering workstations, remote access for third-party entities, human-machine interfaces [HMIs], operator laptop connections)?

PRINCIPLE NOTES

2.5. PRINCIPLE 5: Layered Defenses

KEY QUESTION

How do I create the best compilation of system defenses?

PRINCIPLE OVERVIEW

The best defensive capability for critical consequences is formed by an assemblage of controls, including physics-based analog mitigations, capabilities to protect key system elements, capabilities to detect adverse operating or security conditions, and capabilities to aid in response and remediation. In **Resilient Layered Defenses**, engineers, and their operational cybersecurity support team work together to, for the most critical consequences identified, arrange the best compilation of those defenses to avert the worst impacts from the prioritized consequences. The engineers and operational cybersecurity team work together to ensure that each of the defensive capabilities and services is tuned based on the identified consequences and how the worst impacts of those consequences can be avoided.

QUESTIONS

What layers of digital control defenses (e.g., network segmentation, access control, encryption, etc.) are present in the system?

What layers of engineered control defenses are present in the system?

How are multiple defenses independent of each other such that the failure or compromise of one has no effect on others?

How are critical functions sufficiently protected by layered defenses?

Where are there single points of failure that could result in undesired exposure of the critical function.

How can the team assess and adjust layered defenses to maintain the desired level of protection after system upgrades, configuration changes, requirements changes, or changes in critical consequences?

2.6. PRINCIPLE 6: Active Defense

KEY QUESTION

How do I proactively prepare to defend my system from any threat?

PRINCIPLE OVERVIEW

Planning for **Active Defense** can begin as soon as a conceptual design for a system exists and it continues through the system's retirement. At the design phase, teams can begin to plan how defensive actions should be carried out for the most consequential events. This activity is aided by ensuring that the system designers, operators, and cybersecurity support team discuss the adverse consequences identified and how such events could occur, especially, at the appropriate level of detail for system maturity, the process, or kill chain of how the adverse consequence would manifest within the system. From this discussion, system states and anomalies which might be initial indicators of one of the identified consequences can be identified. Next, plans can be developed for actions to be taken upon detection of an identified indicator. Plans should include points of contact for specific roles and responsibilities across the spectrum of functions associated with the system, since **Active Defense** of the system may require support from a broad set of roles, and they may not all be aware of each other. Once plans are in place, systems should be created to ensure that these plans are regularly practiced, and that the overall approach is regularly assessed to identify emerging consequences, indicators, and opportunities for more advanced defensive approaches.

QUESTIONS

What are the indicators, including the earliest precursors, that a high consequence event could be caused, intentionally or unintentionally?

What temporary operational changes can be made in response to a perceived threat?

What countermeasures, compensating controls, or alternative operations strategies support active defense while maintaining critical functions?

How are active defense features/tools/procedures tested, validated, and regularly exercised during systems operations and are those results representative of how they would be expected to perform?

How are current or new features tested following maintenance, changes, and upgrades?

Who has the documented responsibility and accountability to initiate and terminate active defense measures, and how are they and others notified of an active threat or aware of triggers to temporarily change operations?

2.7. PRINCIPLE 7: Interdependency Evaluation

KEY QUESTION

How do I understand where my system can impact others or be impacted by others?

PRINCIPLE OVERVIEW

All systems have interdependencies, both direct and indirect. While teams regularly consider the risks posed by physical interdependencies in the normal systems engineering processes, they rarely consider how a cyber-attack or digital failure of an interdependent system may affect the system under design.

When evaluating interdependencies from a cyber-informed perspective, evaluate the physical interdependency risks already considered, but judge whether a cyber-attack might make a given consequence more possible or might have the potential to make it more intense than a physically-driven event. Are there functions in the interdependent system not normally accessible to operators which might cause untoward effects on our system if activated? Where might interdependent systems activate command logic on the system under design? Where might automation between the two systems cause cascading effects? In the same vein, where might the system under design be able to affect the interdependent systems in unexpected ways.

QUESTIONS

What supporting utilities (e.g., telecommunications, water, power) provide inputs to the system that are essential for system-level critical function delivery?

What inputs do the system's critical functions require that are not directly and completely controlled by the system

If access to a critical input is lost, can the input be obtained from alternative sources, and/or how will the system continue to execute its critical functions without it?

What outputs does the system provide that are critical inputs to other business systems or infrastructures?

If system outputs to dependent system's critical inputs are lost, can the output be produced from alternate sources?

How are changes in interdependent systems communicated and used to inform the need for additional controls, capabilities, or investments?

2.8. PRINCIPLE 8: Digital Asset Awareness

KEY QUESTION

How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?

PRINCIPLE OVERVIEW

The digitization of our energy infrastructure allows incredible benefits, providing speed and automation of operations not previously possible. However, digital assets and digitized functions have different weaknesses and frailty modes than their analog counterparts. Far beyond simply vulnerabilities to attack, these assets can function or be made to function in ways that their analog counterparts would not, and consideration of these risks is important to ensuring that the defensive measures for a system are cyber informed.

Digital Asset Awareness begins in design, by considering that any digital device is, at its core, a general-purpose computer with specific command logic for its function layered on top. An attacker, or more rarely, a logic failure can subvert this logic and cause the device to ignore input, change values in command logic, or even execute commands or automated logic unexpectedly. The consequences considered earlier in the process can highlight specific impacts we want to mitigate in design, hopefully with controls that are not solely digital in nature.

Secondly, in operations, digital devices require different forms of maintenance, including patching and upgrades and the export of logs and commands stored on the system. To ensure that such systems are maintained in accordance with the function of our system, we must track the devices installed by hardware model, software version, patch version, location, last update, last export, system function, etc. We should also export logs and, if possible, retain them for forensic needs, along with a "gold disk" configuration of the latest software and logic, if needed. This ensures that we understand where the systems are within our processes, what is occurring on them, how they are maintained, and any emerging risks which have been identified as vulnerabilities. It also ensures that we can restore or replace them if needed.

QUESTIONS

Which digital features in a system have the potential to cause high consequences events from adversarial manipulation or control?

How are digital feature abuse/misuse scenarios used to identify high consequences events, inform requirements for what the system must be designed to not do, and drive digital and non-digital (i.e., engineered controls) mechanisms to prevent abuse/misuse?

How do abuse/misuse scenarios inform operators' thinking about systems and affect system requirements?

What processes ensure that digital assets are tracked and that third-party vendors provide the specifications needed to enable asset tracking?

What processes ensure that operations and maintenance activities (e.g., changes to software, logic, or configurations) appropriately trigger updates to asset tracking records?

What is the process to ensure that applied packages from updates/patches are necessary, desired, and make all the changes promised (and only the changes promised; no new unexpected features introduced)?

Where updates or patching are delayed or not performed, are there alternate defenses that could be implemented to limit impacts of the resulting vulnerability or related exploitations?

PRINCIPLE NOTES

2.9. PRINCIPLE 9: Cyber-Secure Supply Chain Controls

KEY QUESTION

How do I ensure my providers deliver the security the system needs?

PRINCIPLE OVERVIEW

Even at the early design phases, engineers can begin to establish the core security features and assumptions which should be implemented by every supplier bringing components or services into the system. These may include guidelines about required features in digital systems, limits on where such systems can be acquired, and how updates must be verified and signed. They may include practices for vendor behavior when providing onsite or remote maintenance. They may include requirements for sharing information about cyber incidents, vulnerabilities, bills of materials, and vendor development processes. Each of these controls contributes to the overall supply chain security of the system. These requirements should be discussed with the roles who may have a responsibility for ensuring them, including procurement, cybersecurity, and system operators.

For each control or feature, the team should consider how it will be verified, when it can be verified and how often, and who can perform the verification (procurement, cybersecurity, operators, etc.). These processes should be built into requirements for development and operations of the system, and verification should occur more than once for controls which could change or erode over time. The controls devised by the engineering team should be complimentary to those leveraged by the organization's purchasing and cybersecurity processes, but because they are drawn from potential catastrophic system consequences, they may well exceed the general due diligence performed by the organization.

QUESTIONS

What assumptions have been made about the availability, quality, and security of the products or services that are critical to system functions or to the mitigation of high consequence events?

How can the organization reduce supply chain risk by prioritizing familiar technologies, technologies that are expected to be continuously available, and suppliers with a strong history of meeting supply chain constraints?

How are delivery interruptions of critical components avoided by using alternate methods of delivery or by arranging for multiple alternate sources?

How does the organization ensure the services and components that are critical to system function are being used in alignment with the vendor's intended purpose to minimize consequences of disruption, the expected security functions and requirements, and the vendor's responsibility and accountability in mitigating and preventing disruptions?

How will the organization identify and manage the risks of continued use of a component or subcomponent if a vendor support contract expires?

2.10. PRINCIPLE 10: Planned Resilience

KEY QUESTION

How do I turn "what ifs" into "even ifs"?

PRINCIPLE OVERVIEW

You can imagine the general operating mode of a system, with all functions available and working as expected; however, resilience requires that we imagine and plan for different kinds of failure modes of a system, ideally including those linked to the set of prioritized undesired consequences created earlier. We must understand these failure modes, including how to operate through them, albeit at a lower level of performance or reliability. Ideally, a set of diminished operating modes can be created which, though not ideal, can be built into expectations for well-understood modes of operation. Within each diminished operating mode, plans can be made for what would cause that mode, how that mode would function, and the changes to staff, systems, safety guidelines, performance, or other system conditions when it is assumed. Once part of our overall set of system operating modes, it is reasonable to train, exercise, and assess our performance in each of these diminished modes on a regular basis.

These resilient diminished operating modes should include modes assumed because of a digital failure or cyber-attack. For any critical system, diminished operating modes should include operations during an expected cyber-attack involving one or several of those systems, operating when the team is uncertain of the validity of the data emerging from the system, where critical automation logic is not dependable, or where core network connections or support services are not available. It is likely that exercising these modes will require the operations team to pair with cybersecurity counterparts and understand the roles and responsibilities each will perform. Considering these operating modes may also require that the team consider altering the system design to allow limited manual operations options when digital systems are not operating or trusted. Note that a capability may be restored to diminished operation via use of an alternate mechanism or supply source.

Considerations for **planned resilience** should also include how untrusted systems can be restored to full function within the system context, including what operational steps will be required to ensure future trust, or whether that is possible given the function of the system or component.

QUESTIONS

What are the limits of acceptable degradation for critical system functions and what alternate operating modes would protect and maintain those critical system functions within acceptable limits?

How reliable are the supporting utilities (e.g., power, communication) and what plans are in place for continued operation if one or more is lost?

How does the system maintain safety, security, and/or stable operation in the case of partial or complete functional failures (i.e., fail-secure, similar to fail-safe)?

Do processes controlled by an automated system have a manual operation mode that is practiced and has been verified to have no dependencies on automation?

How does the organization maintain business continuity and critical function delivery through incident response and recovery?

How will resilience measures be validated?

How do you practice and continually improve response and recovery processes?

PRINCIPLE NOTES

2.11. PRINCIPLE 11: Engineering Information Control

KEY QUESTION

How do I manage knowledge about my system? How do I keep it out of the wrong hands?

PRINCIPLE OVERVIEW

From the first conception of a system until its retirement, immense amounts of information are created about how the system is designed, the elements and components within it, the skills required to operate it, its performance, procedures for maintenance and operations, and more. This information, in the wrong hands, can aid an adversary to understand system weaknesses, existing component vulnerabilities, and even human targets to aid in planning their attack. This information can be released during procurement processes, often shared via public release to ensure an open and fair competitive process. It can be released in job listings, where specific technical criteria are used to find good employment candidates but may also tip an adversary to system features or vulnerabilities. It can be shared in news articles or success stories about the system's entry to operations, where even a system photograph may release information helpful to an adversary.

During the system design process, the engineering team can begin to identify, using the prioritized list of consequences developed earlier, the specific information which would be of most value to an adversary to enact an undesired consequence. They can develop administrative processes for protecting the information, determining who can possess it, how to prevent inadvertent duplication and sharing, how to remove access, how to review and approve information release, how to ensure team members understand the sensitivity of the information they have access to, and how to protect it, etc. Because engineering systems are in active use, sometimes for decades, it is crucial that even the earliest information about the system design be protected throughout the lifecycle of the system.

QUESTIONS

What information about the system (e.g., requirements, procurement, engineering diagrams, processes and procedures) is sensitive and how is that information protected?

How are internal stakeholders trained and held accountable to ensure potentially sensitive information is correctly identified and protected?

How are data sensitivity controls and requirements passed to external stakeholders (e.g., subcontractors, service providers, distributors) and enforced through contracts, procurement, and reporting documents?

How are internal stakeholder roles and associated access privileges defined and adjudicated to enable necessary access to sensitive system data? Do information security policies that overly constrain workflows "encourage" workarounds and bypasses?

Could an adversary reasonably derive sensitive system information from hiring, recruitment, marketing or other externally facing information sources?

2.12. PRINCIPLE 12: Organizational Culture

KEY QUESTION

How do I ensure that everyone's behavior and decisions align with our security goals?

PRINCIPLE OVERVIEW

Shared beliefs, perspectives, and values about cybersecurity determine how a group will prioritize investments and actions to improve its realization. For a culture which does not value cybersecurity, whether they see it as an unnecessary expense, a low risk or impact, or an impediment to productivity, there will not be a desire to invest in people, processes, and technology to provide cybersecurity. An engineering design team, cognizant of the consequences of digital failure or cyber-attack on a system under design, has a core responsibility to aid the entire set of stakeholders who are accountable, responsible, consulted, or informed about the system to understand the need for cybersecurity and how each stakeholder's role can affect, both positively and negatively, the overall security of the system.

To build a culture of cybersecurity around the system design process, engineering design teams can emulate best practices for building a safety culture. These include having regular discussions about how and why cybersecurity is incorporated into the system, recognizing and celebrating good decisions and right actions of team members, and treating failures as opportunities for learning and improvement. Because team members external to the design process may not recognize how their job role can contribute to or diminish the cybersecurity of the overall system, it is important for the design team to personalize conversations to the individual. As discussed earlier under **supply chain controls**, these discussions should extend to everyone involved with the system, even a subcontractor or external service provider. Each person interacting with the system should understand the importance of ensuring its security and how their role contributes to that function.

QUESTIONS

How do expectations around creating, operating, and maintaining the system transfer from the organization to supporting organizations (e.g., hardware vendors, consulting engineers)?

How can choices that make the organization less resilient or bring on undue complexity/cost (e.g. delaying hardware and software life-cycle updates) be recognized and documented?

What assumptions are made about existing skill and experience and what training, education, and practice will be needed for those who will operate, maintain, secure, and defend the system?

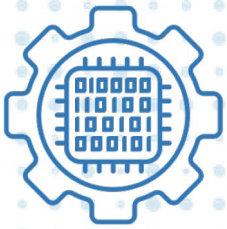
How is interpersonal trust maintained across the entire organization?

What processes ensure that operators consider the possibility of digital sabotage when responding to and diagnosing process anomalies?

How can the organization foster a culture of timely reporting of issues in people, process, and technology without fear of reprisal, and with confidence that the issues will be addressed?

How can the organization positively reinforce behaviors and choices that support security outcomes, while reducing those that harm security outcomes?

PRINCIPLE NOTES



Cyber-Informed Engineering

Idaho National Laboratory