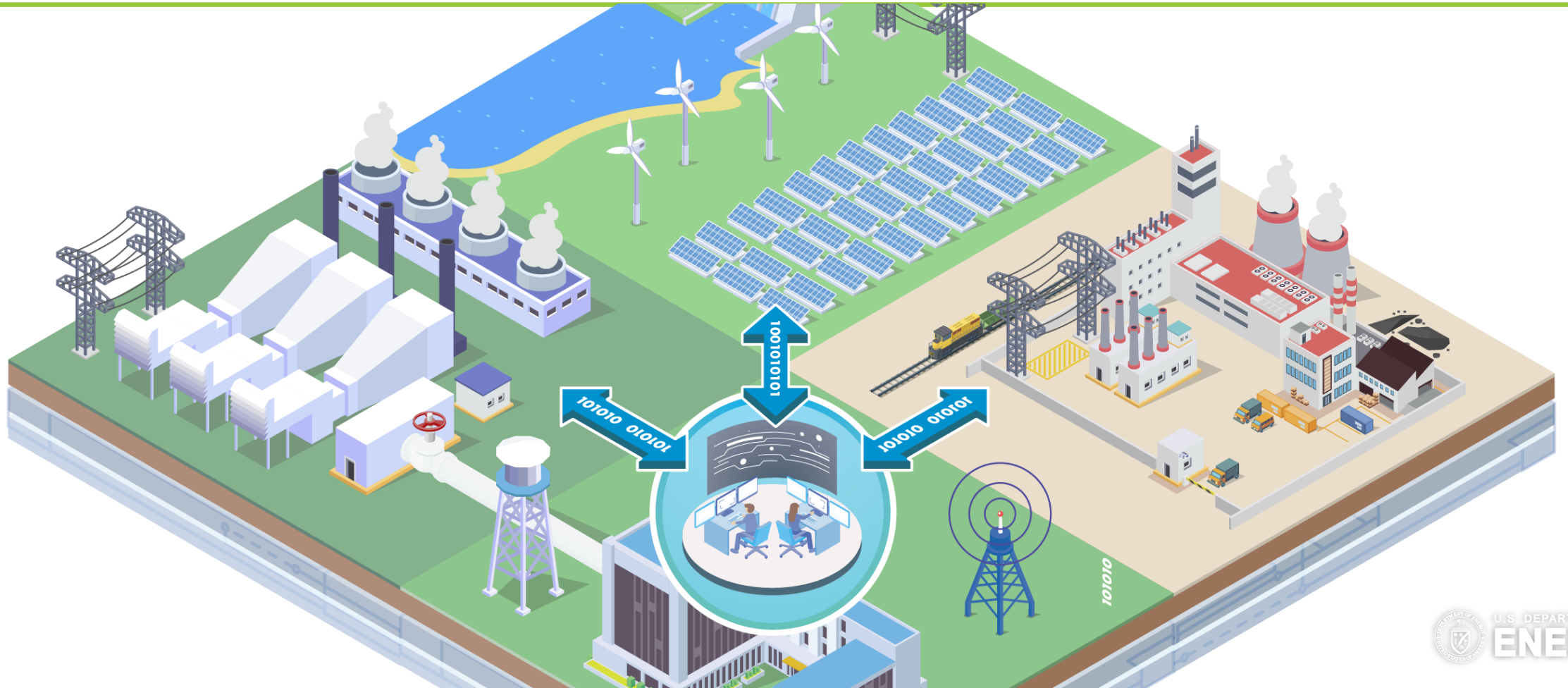
Cyber Security Lifecycle Risk Reduction Framework

NATIONAL ENERGY TECHNOLOGY LABORATORY

2020 SENSORS AND CONTROLS PROJECT REVIEW MEETING



U.S. DEPARTMENT OF ENERGY

Purpose of the Project

Cyber Security Lifecycle Risk Reduction Framework

What are the lifecycle considerations that effect cyber security?

- Can strategies be optimized based on plant lifecycle, component lifecycle, and time in year (demand)?
- Can cyber security controls be selected so they require less effort to maintain effectiveness?

What are the current risk reduction best practices?

- NERC CIP
- NIST Publications
- TAM/CCE
- Others?

What are the research gaps for cyber security?

- Lack of industry accepted methods?
- Lack of technology and tools, resulting in manual process?

Cyber Security Challenges

Unique Challenges and Drivers to Generation OT

1

Changing Expectations

- Regulations
- Government Direction
- External Stakeholders
- Internal Stakeholders

2

Changing Technology

- Additional Sensor Technology
- Advanced Monitoring and Diagnostics
- Cloud and virtualization
- IT/OT/IoT
- Product end of life (suppliers and sub-suppliers)

3

Applying a Graded Approach

- Enhanced program beyond minimum threshold
- Targeted approach → greater efficiencies
- Cost benefit justification for decision makers
- System understanding

4

Asset Management

- Level of granularity needed vs what is commonly available
- Limitations on OT Capabilities
- Non-networked assets

Enabling a Secure Digital Transformation in Fossil Power

Expected Benefits of Research

Cyber Security Lifecycle Risk Reduction Framework

Framework

- Process for holistic risk informed cyber engineering
- Select best tools for your specific environment
- Considerations based on real world experience

Best Practices

- Practical use cases and lessons learned
- Methodologies and standards that can be integrated into program

Research Gaps

- Future research needs for fossil generation

Industry Collaboration and Validation

Cyber Security Lifecycle Risk Reduction Framework

EPRI
Jeremy Lawrence – PI/Project PM
Jason Hollern – Technical SME

Southern Engineering Services
Brad Geddes – PI
Bruce Geddes – Technical SME

Idaho National Laboratory
Dr. Craig Rieger – PI
Jake Gentle – Technical SME
Sarah Freeman – Technical SME

Department of Energy – National Energy Technology Lab (NETL)
Barbara Carney – DOE PM

- Southern Company
- Duke Energy
- Exelon
- WEC Energy Group
- Oglethorpe Power Company
- Prairie State Generating Company
- Tri-State Generation and Transmission
- Emerson
- Schneider Electric/Framatome
- Schweitzer Engineering Laboratories (SEL)

How to use this Framework

Cyber Security Lifecycle Risk Reduction Framework

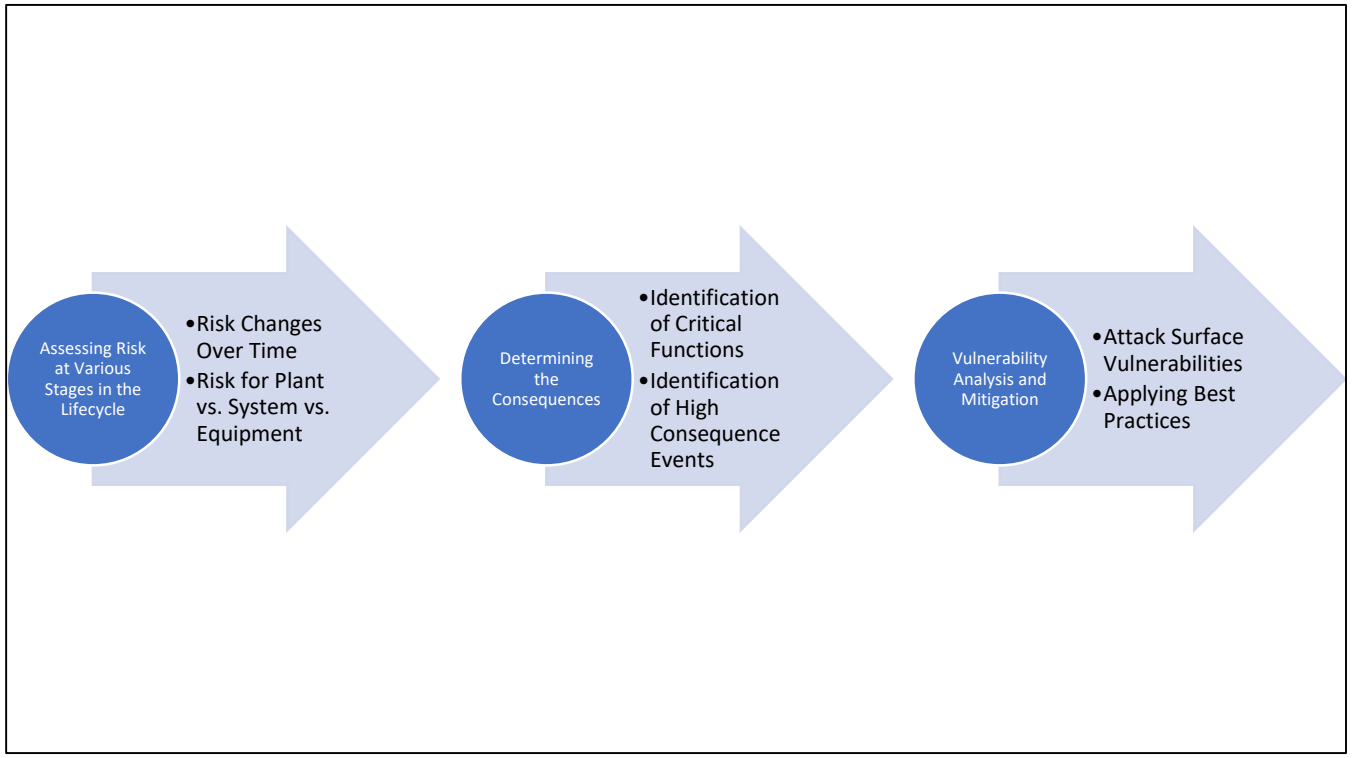
Framework structure:

- Phase 1: Temporal risk determination
  - Plant, systems, and equipment
- Phase 2: Consequence identification
  - Critical functions and high consequence events
- Phase 3: Vulnerability analysis and mitigation
  - Attack surface vulnerabilities and applying best practices

Gap analysis and research opportunities

Appendix A

- Tool kit



Temporal Nature of Lifecycles

Cyber Security Lifecycle Risk Reduction Framework

Utility Lifecycle

- Load, weather, cost, amortization, financial forecasts, etc.

Plant Lifecycle

- Designed lifetime, age, life extension, end of life

Plant System and Component Lifecycles

- Equipment aging, repair/replace, obsolescence, O&M capability, etc.

Vendor Lifecycles

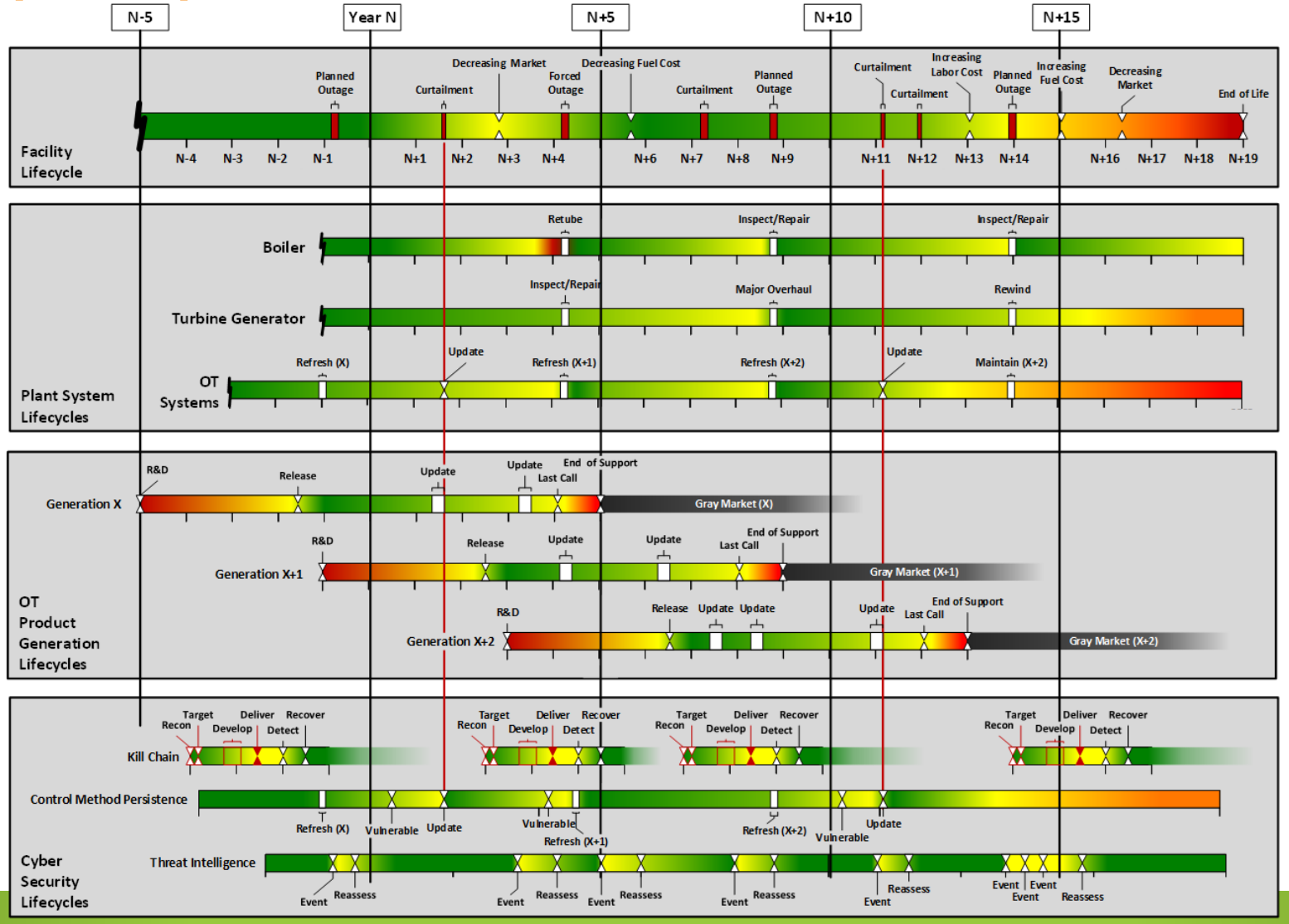
- Strategy, R&D, updates, product generations, last calls, support, etc.

Cyber Security Lifecycles

- Discoveries, threat capabilities, kill chains, controls persistence, etc.

Lifecycle Influences

Cyber Security Lifecycle Risk Reduction Framework



Consequence ID and Prioritization

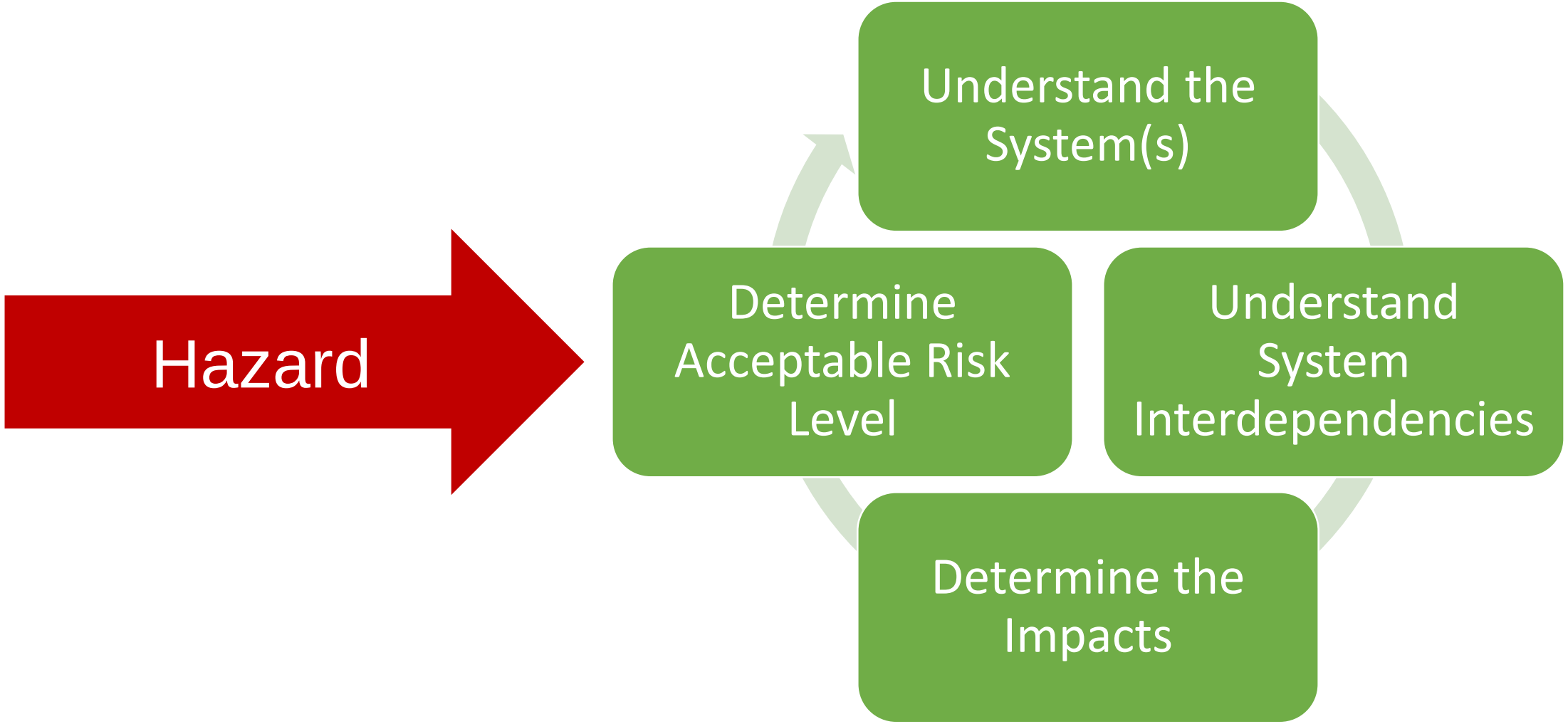
Cyber Security Lifecycle Risk Reduction Framework

In this report, a hazard is a system condition, which if exploited, can lead to a consequence.

A hazard analysis may identify different digital systems that contribute to different hazards and may yield different acceptable risk levels based on the hazard.

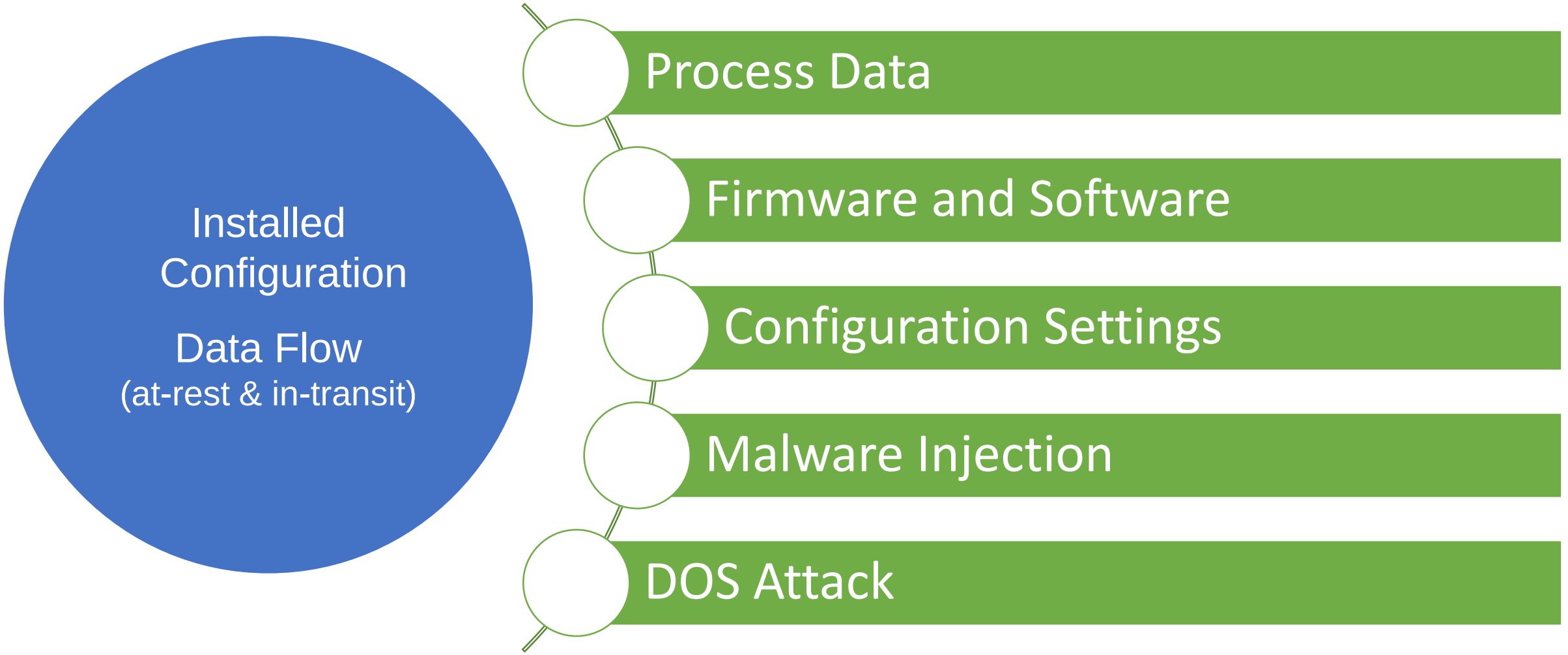
An owner may analyze for different hazards with different consequences

Cyber Security Lifecycle Risk Reduction Framework



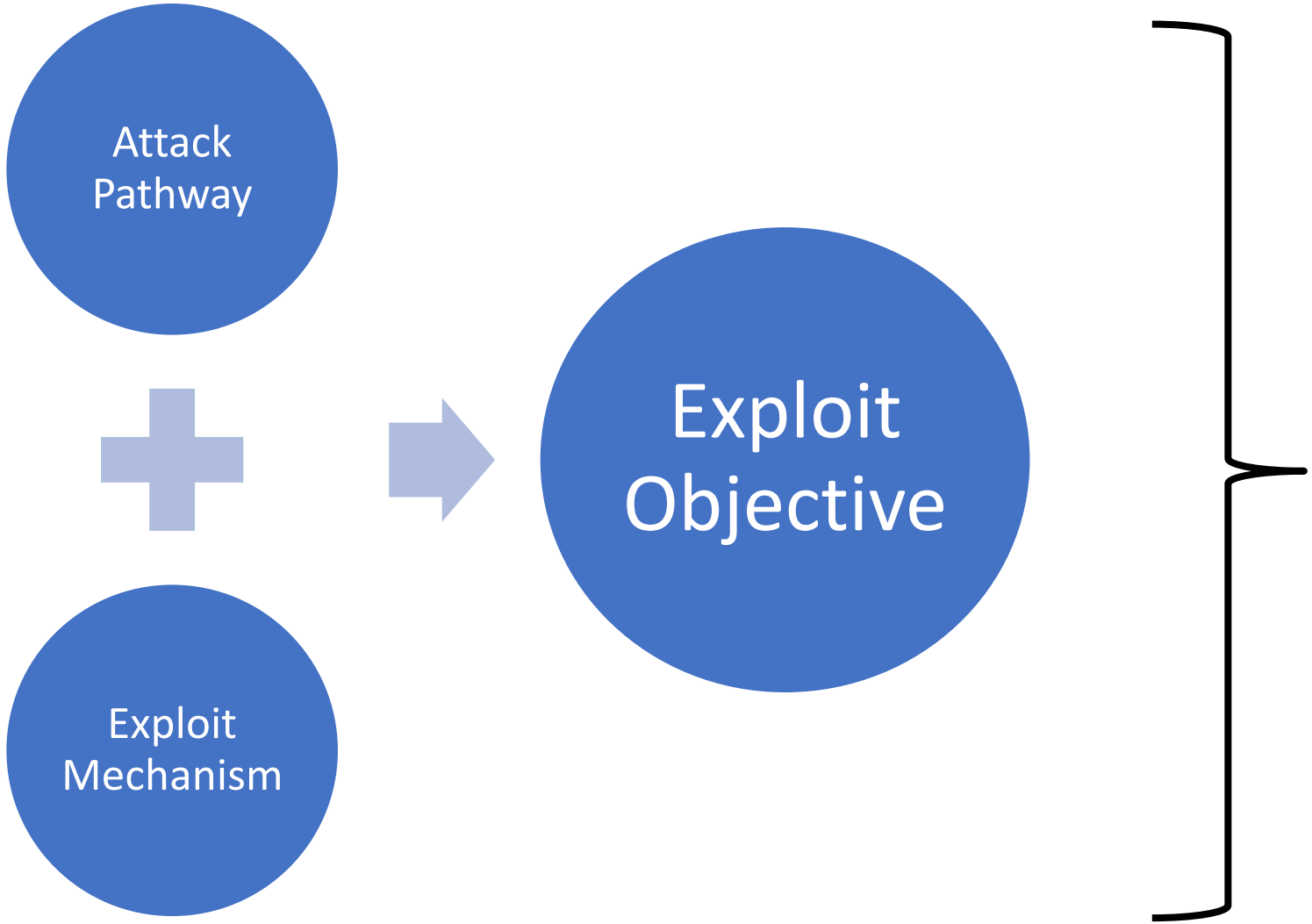
Attack Surface Exploit Objectives

Cyber Security Lifecycle Risk Reduction Framework



Attack Surface Characterization

Cyber Security Lifecycle Risk Reduction Framework



Exploit Sequence

Attackers must traverse existing exploit sequences

Cyber Security Lifecycle Risk Reduction Framework

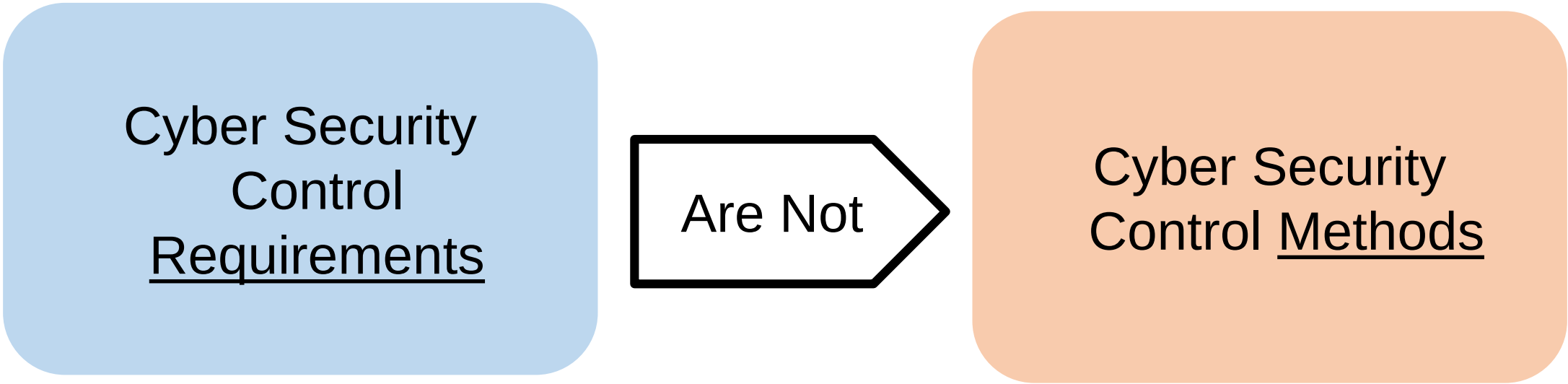
Most cost-effective and sustainable security control methods to

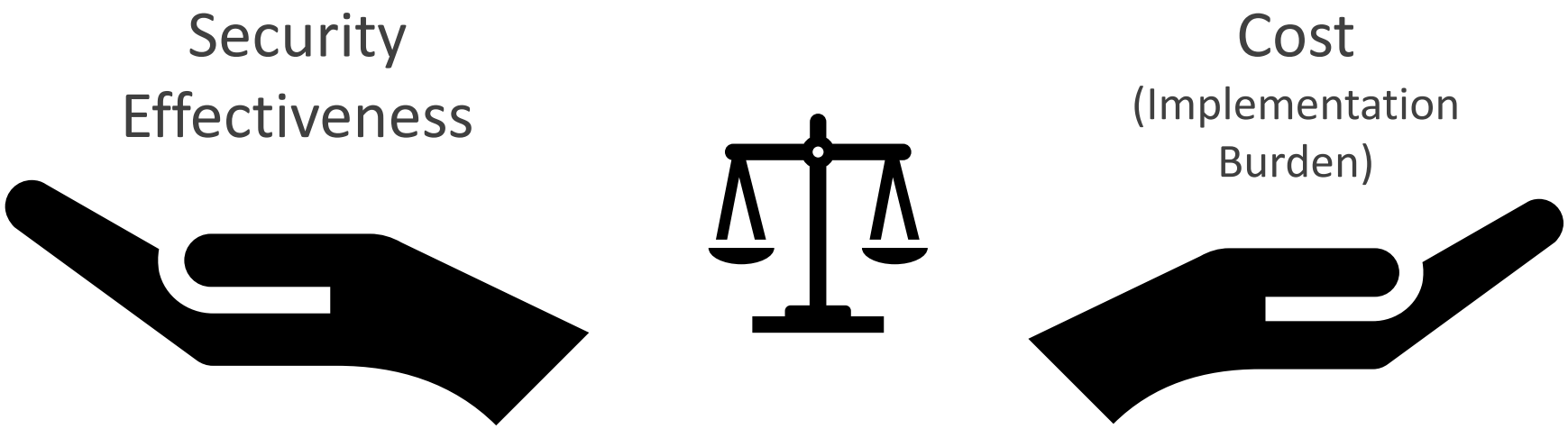
Mitigate an attack surface to an acceptable risk level.

Best practice mitigation uses the principles of the NIST Framework

- Identify
- Protect
- Detect
- Respond & Recover

Cyber Security Lifecycle Risk Reduction Framework





Systems engineering best practice allows an owner to choose between technical options to balance security effectiveness and cost to achieve an acceptable business outcome.

Incorporating Risk

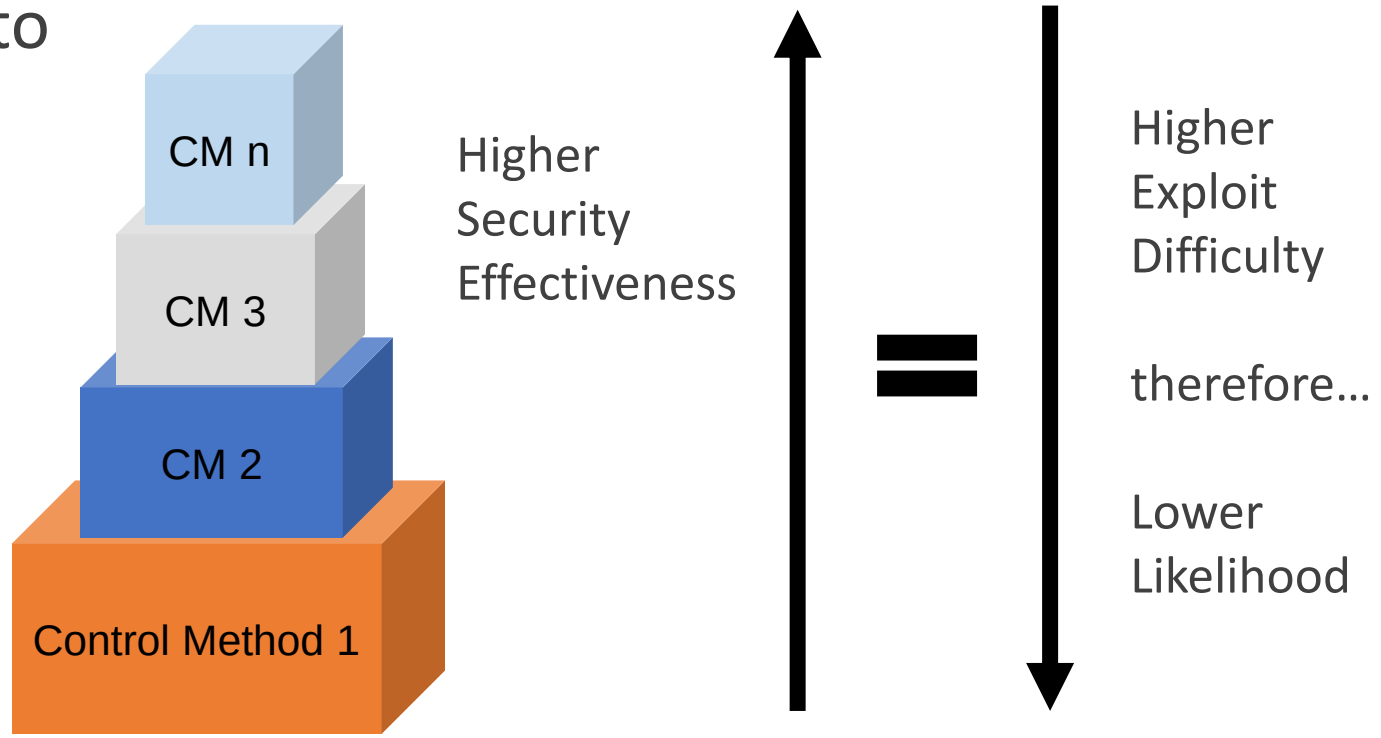
Cyber Security Lifecycle Risk Reduction Framework

Exploit Difficulty
Inverse of "Likelihood"

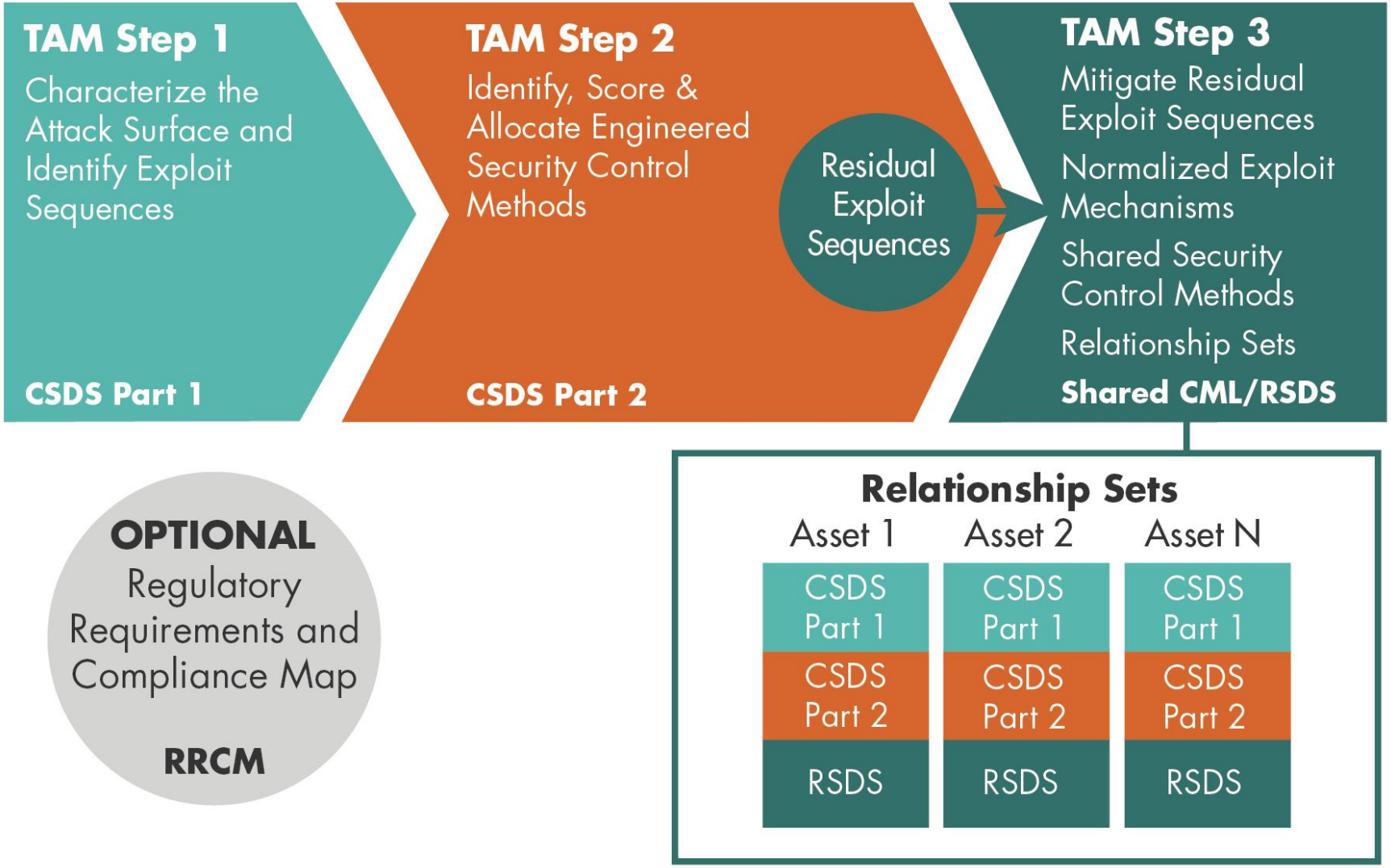
How difficult is it for an adversary to overcome a control method?

Qualitatively Score Control Methods and Consequence

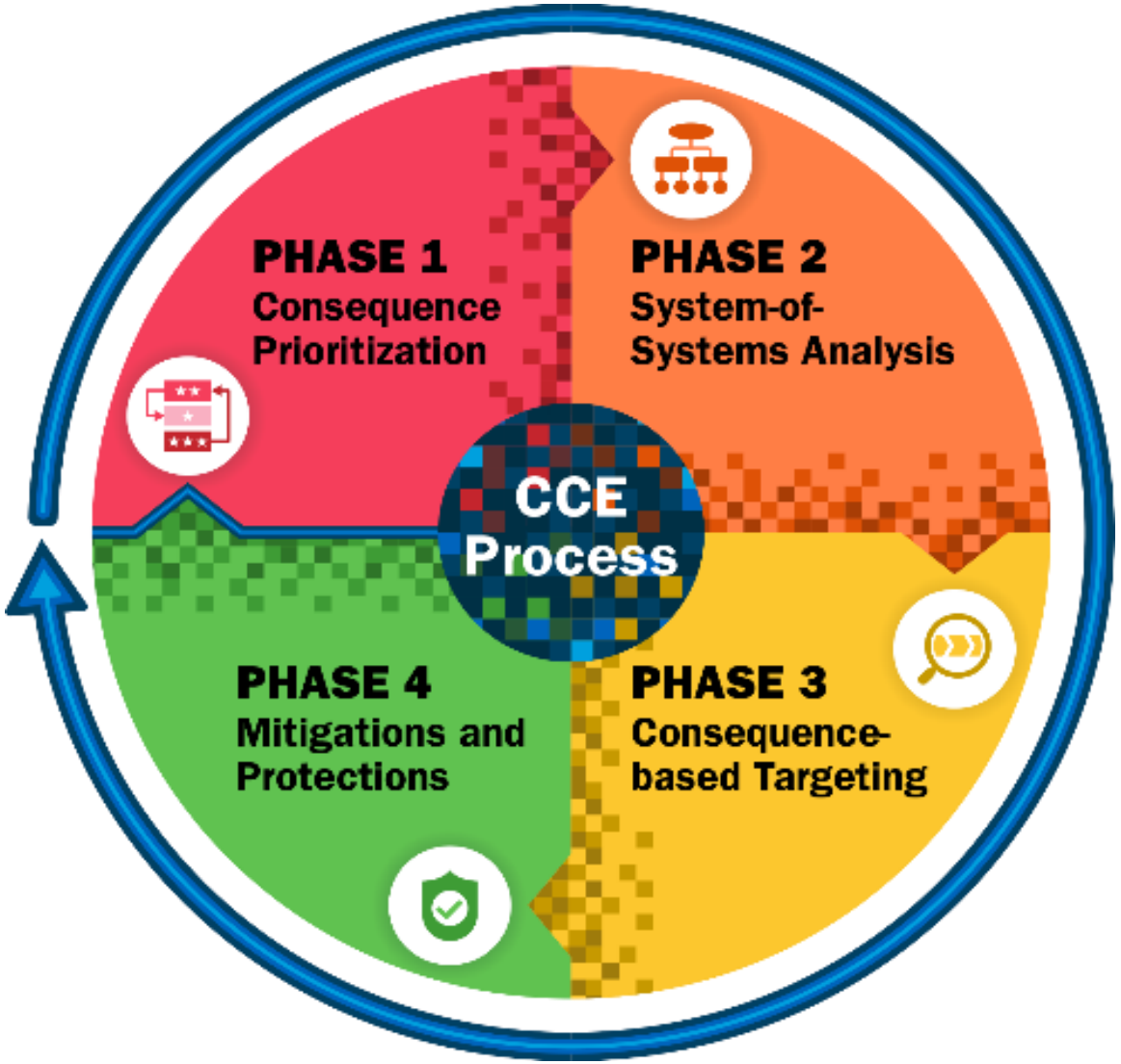
- Score Control Methods
- Allocate Control Methods to each Exploit Sequence
- For each Security Function
- Reduce likelihood to acceptable level
- For a given consequence
- Adjust for lifecycle



TAM as a Best Practice Strategy



CCE as a Best Practice Strategy



Success Stories

Southern Nuclear Plant Vogtle recognized for advancements in cybersecurity

EPRI ELECTRIC POWER RESEARCH INSTITUTE

SUCCESS STORY

CONED AND DUKE ENERGY EVALUATE CYBER SECURITY WITH TECHNICAL ASSESSMENT METHODOLOGY

https://www.southerncompany.com/our-companies/southern-nuclear/southern-nuclear-news-stories/epriaward-200316.html

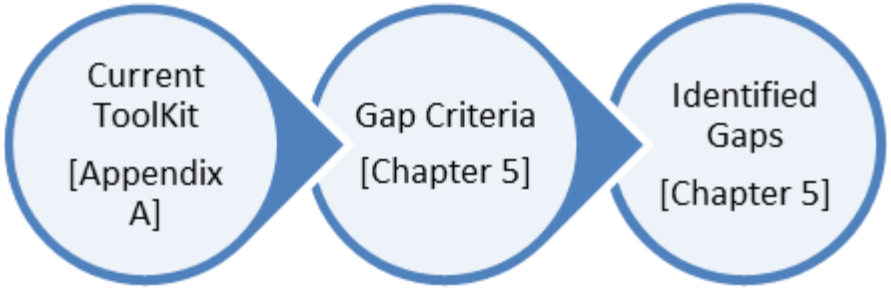
"These remarkable efforts at Plant Vogtle demonstrate the innovation and determination of this team to *build advanced processes that are both efficient and effective* in combatting a global cybersecurity threat to our nation's infrastructure," said Tom Wilson, chief information security officer for Southern Company.

https://www.osisoft.com/presentations/security-and-hardening-of-your-pi-system/

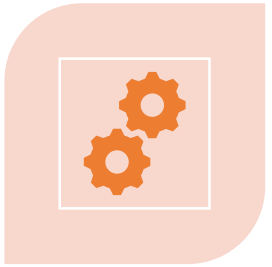
https://www.epri.com/#/pages/product/000000003002017737

https://www.epri.com/#/pages/product/3002017786/

Future Research Recommendations



- Relies heavily on people to execute
- Components that are not inherently secured or need significant resources to secure
- High barrier of entry, either relating to capital cost, knowledge, and/or resource time to implement
- Existing challenges in industry



ASSET AND CONFIGURATION MANAGEMENT

SECURE CONFIGURATIONS FOR OT ASSETS

EVENT RESPONSE

IMPROVED TESTING FOR THE SUPPLY CHAIN