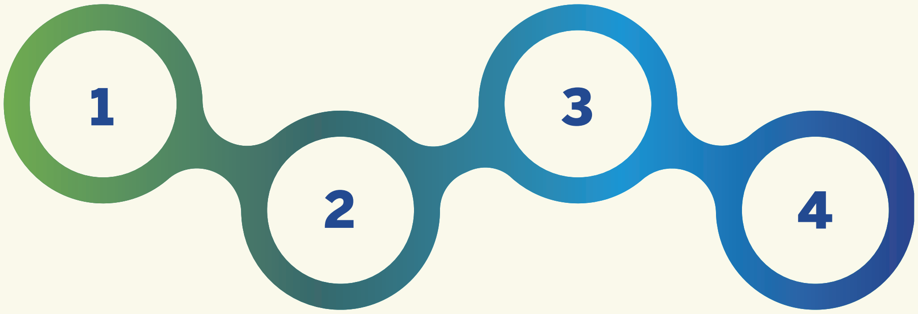


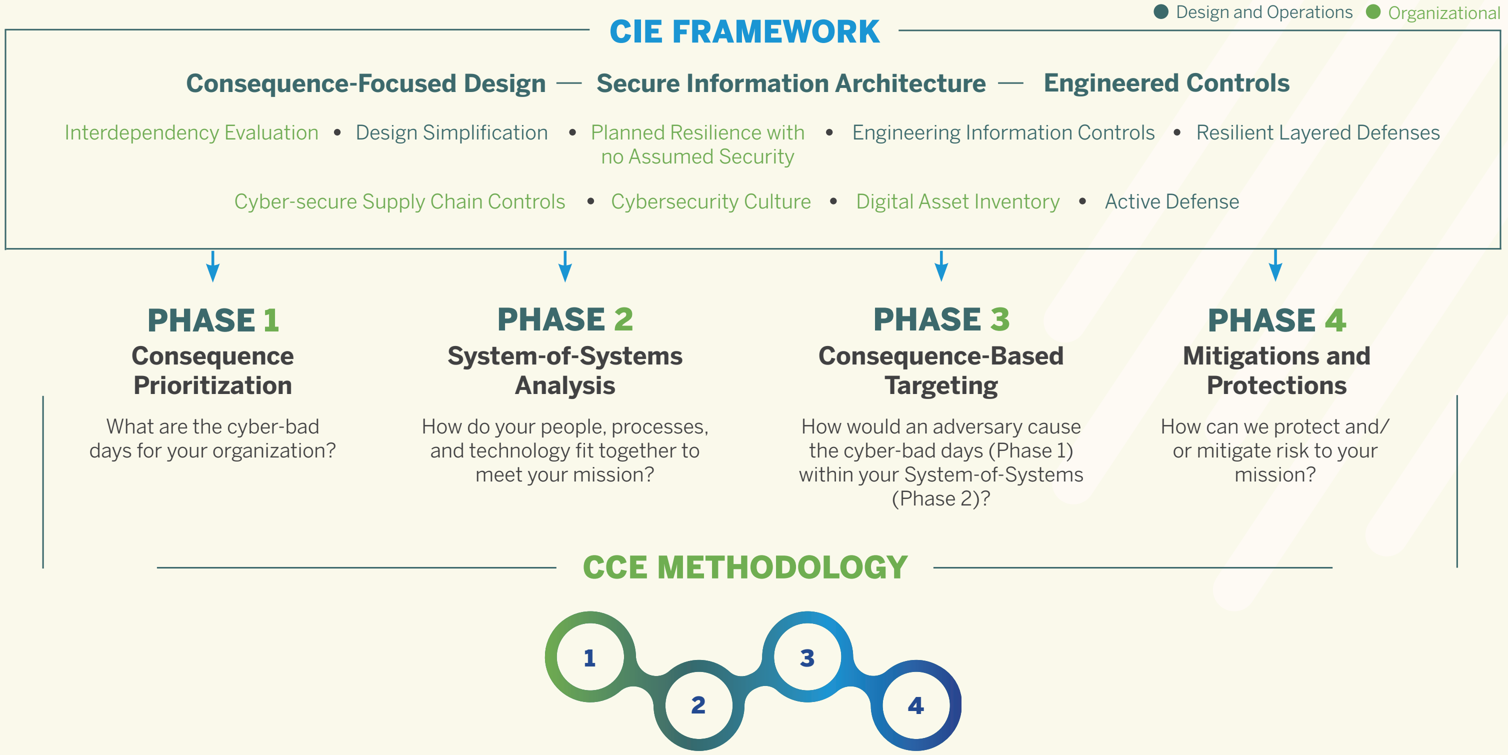
Consequence-driven, Cyber-informed Engineering **(CCE)** & Cyber-informed Engineering **(CIE)**

West Yost has been working with our clients since 2020 to incorporate CCE and CIE into their engineered systems. Through this method, we can effectively **engineer out** current and future cyber risk from their systems.

WEST YOST
Water. Engineered.

INL Idaho National Laboratory

American Water Works Association



● Design and Operations ● Organizational

CIE FRAMEWORK

Consequence-Focused Design — Secure Information Architecture — Engineered Controls

Interdependency Evaluation • Design Simplification • Planned Resilience with no Assumed Security • Engineering Information Controls • Resilient Layered Defenses

Cyber-secure Supply Chain Controls • Cybersecurity Culture • Digital Asset Inventory • Active Defense

PHASE 1
Consequence Prioritization

What are the cyber-bad days for your organization?

PHASE 2
System-of-Systems Analysis

How do your people, processes, and technology fit together to meet your mission?

PHASE 3
Consequence-Based Targeting

How would an adversary cause the cyber-bad days (Phase 1) within your System-of-Systems (Phase 2)?

PHASE 4
Mitigations and Protections

How can we protect and/or mitigate risk to your mission?

CCE METHODOLOGY

> CCE and CIE were developed by INL to improve the cyber-resilience of our critical infrastructure. West Yost is leading the application of both CCE and CIE in the Water Sector. **West Yost is INL's first licensed CCE Partner!**

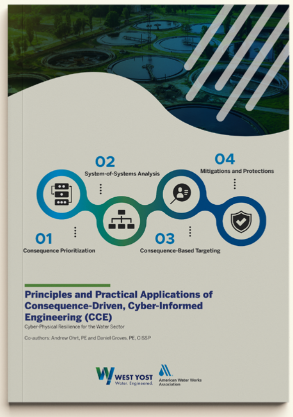
Please contact **Andrew Ohrt, PE** at 952-303-9905 or aohrt@westyost.com for more information.

Fundamental Questions:

1. Do our facilities provide us the manual operability and do our staff have the skills we need to continue to serve our customers – or at least enough to prevent catastrophic failure?
2. How should we account for cyber-risk in our designs to reduce the consequences of a compromised control system?
3. How will we recognize and respond to a compromised system?
4. What engineering, management, and operations principles and practices need to be adopted to reduce the consequences of this threat?

Opportunities to implement CIE/CCE within your organization:

- Conduct a CCE assessment on current systems.
- Conduct CIE assessments within the design process for new assets.
- Conduct a CIE assessment on current organizational cyber-risk management practices.
- Train staff on how to implement CCE within your organization.



02 System-of-Systems Analysis

04 Mitigations and Protections

01 Consequence Prioritization

03 Consequence-Based Targeting

Principles and Practical Applications of Consequence-Driven, Cyber-Informed Engineering (CCE)

Cyber-Physical Resilience for the Water Sector

Co-authors: Andrew Ohrt, PE and Daniel Groves, PE, CISSP

WEST YOST Water. Engineered.

American Water Works Association

West Yost is currently working with **AWWA** to write the book on CCE in the Water Sector! We expect to publish by mid-2023.

www.westyost.com **www.watercce.io**

Principles and Practical Applications of Consequence-Driven, Cyber-Informed Engineering (CCE)

Cyber-Physical Resilience for the Water Sector

Co-authors: Andrew Ohrt, PE and Daniel Groves, PE, CISSP

WEST YOST Water. Engineered.

American Water Works Association

02 System-of-Systems Analysis

04 Mitigations a

01 Consequence Prioritization

03 Consequence-Based Targeting

Principles and Practical Applications of Consequence-Driven, Cyber-Informed Engineering (CCE)

Cyber-Physical Resilience for the Water Sector

Co-authors: Andrew Ohrt, PE and Daniel Groves, PE, CISSP

WEST YOST Water. Engineered.

American Water Works Association

WEST YOST
Water. Engineered.

INL Idaho National Laboratory

American Water Works Association