



# Responsible Use of Cloud Solutions - Community of Practice Meeting

April 2025

*Changing the World's Energy Future*

Julia Catherine Morgan, Emma Mary Stewart, Abby M. Neumann



**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.

# **Responsible Use of Cloud Solutions - Community of Practice Meeting**

**Julia Catherine Morgan, Emma Mary Stewart, Abby M. Neumann**

**April 2025**

**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**



# Responsible Use of Cloud Solutions

## Enabling Resilient Reliable Secure Cloud Deployments

DOE GDO Project  
COP Meeting 3

Emma Stewart (INL) – Julia Morgan and Abby Neumann  
GDO PM: James Briones (DOE), Jessica Whitaker (DOE)

# Goal & Schedule – Community Of Practice

- Bring technical and strategy like minded folks together to talk about framework direction and advise
- Cirrus technical team will bring part of the framework being developed to each discussion
- 15 mins of discussion/input on a problem
  
- **OUTLINE**
  - How is Cyber-Informed Engineering applied in Cirrus?
  - Ideas
    - Talk about Cyber-Informed Engineering (CIE)
    - CIE in Cirrus
    - CIE Analysis Output
    - User Interface Updates
  - Timing of next COP

# Framework Design Principles

Consequence-Driven

Cost/Benefit at every layer of analysis

Tailored to stakeholder user and type – critical functions

Forward looking

Applicable to emerging use cases in grid and digital modernization

**Cyber-Informed**

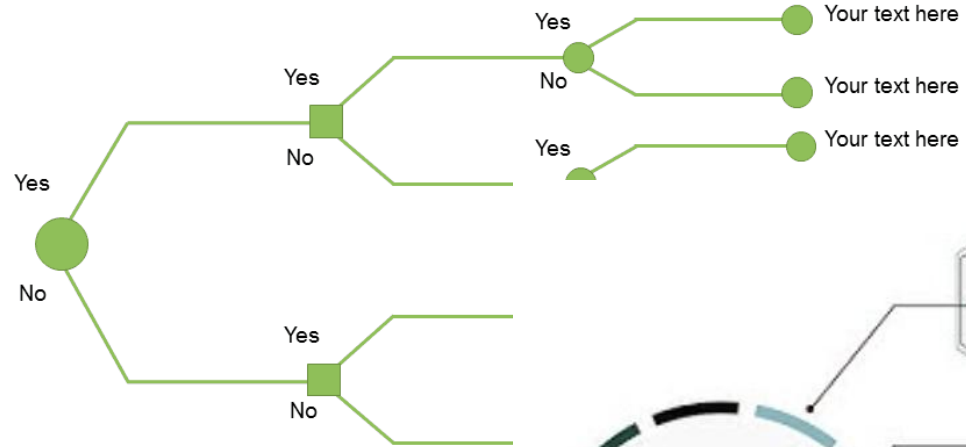
Explainable

Repeatable

Enable ability to unlock potential modernization paths

# Goal of Cirrus

- Develop & Test a consequence driven **decision support framework** for
- Dynamic assessment for entities to strategize their grid **modernization deployment strategy** in the cloud
- Test against use cases & partner users enabling adequate assessment of deployment plans



Idaho National Laboratory

HOME ABOUT RESEARCH

Critical Infrastructure Protection | Wireless Programs | Defense Systems | Nuclear Security and Energy

**Cyber-Informed Engineering (CIE) builds tools for high-level implementation, certification and curriculum accreditation.**

CIE is the result of constant evaluation of engineers and technical staff not capitalizing on opportunities to address risk. This late-stage mitigation of risk leaves gaps which an ever-advancing adversary is well aware of. CIE proactively secures existing digital infrastructure and builds new systems designed to withstand the modern threat environment.

The DOE Office for Office of Cybersecurity, Energy Security, and Emergency Response (CESER) sponsors INL CIE initiatives and coordinates the CIE program that includes Idaho National Laboratory (INL); the National Renewable Energy Laboratory (NREL), and industry, academic, and other partners in support of the Department of Energy's National Cyber-Informed Engineering Strategy, and the National Cybersecurity Strategy.



## Implementing the Cyber-Informed Engineering Strategy

**CIE Resource Library**

[Learn More](#)

*Cyber-Informed Engineering*  
**Implementation Guide**  
Version 1.0

**CIE Implementation Guide**

[Learn More](#)

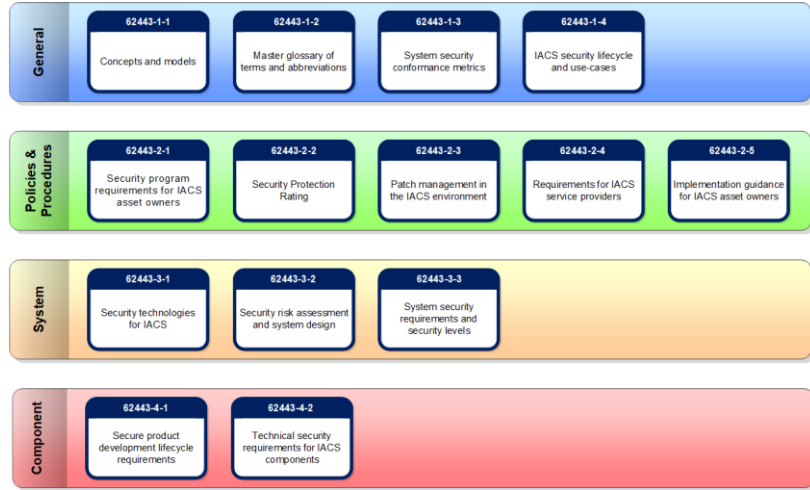
# Cyber-Informed Engineering (CIE)

- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact.
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to create a **culture of security** aligned with the existing industry safety culture.

# Cyber-Informed Engineering (CIE)

PRINCIPLE	KEY QUESTION
<b>Consequence-Focused Design</b>	How do I understand what critical functions my system must <u>ensure</u> and the undesired consequences it must <u>prevent</u> ?
<b>Engineered Controls</b>	How do I implement controls to reduce avenues for attack or the damage which could result?
<b>Secure Information Architecture</b>	How do I prevent undesired manipulation of important data?
<b>Design Simplification</b>	How do I determine what features of my system are not absolutely necessary?
<b>Layered Defenses</b>	How do I create the best compilation of system defenses?
<b>Active Defense</b>	How do I proactively prepare to defend my system from any threat?
<b>Interdependency Evaluation</b>	How do I understand where my system can impact others or be impacted by others?
<b>Digital Asset Awareness</b>	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?
<b>Cyber-Secure Supply Chain Controls</b>	How do I ensure my providers deliver the security we need?
<b>Planned Resilience</b>	How do I turn “what ifs” into “even ifs”?
<b>Engineering Information Control</b>	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
<b>Cybersecurity Culture</b>	How do I ensure that everyone performs their role aligned with our security goals?

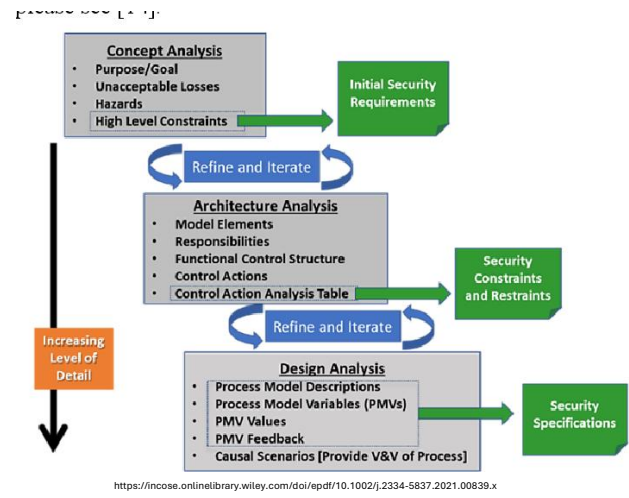
# OK, But How Do You CIE?



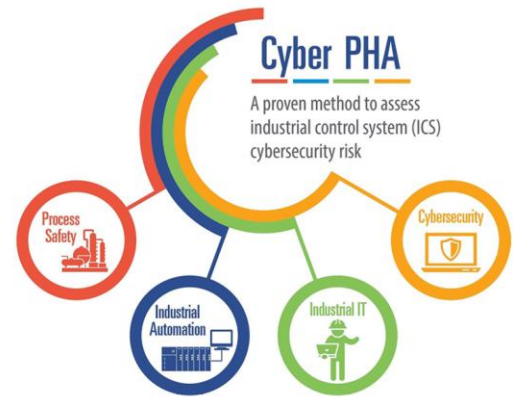
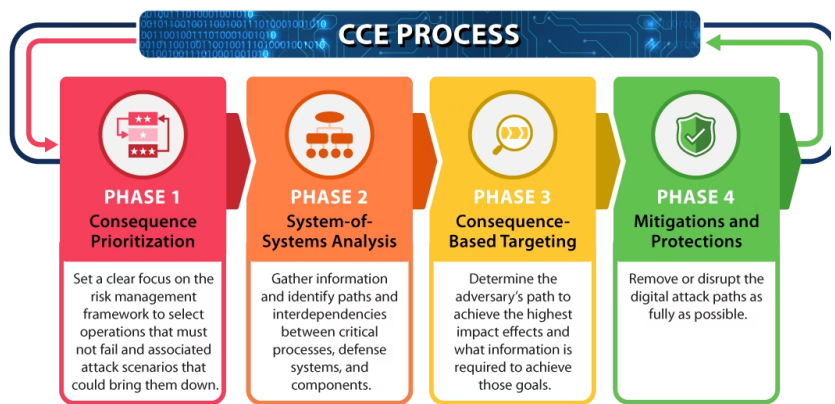
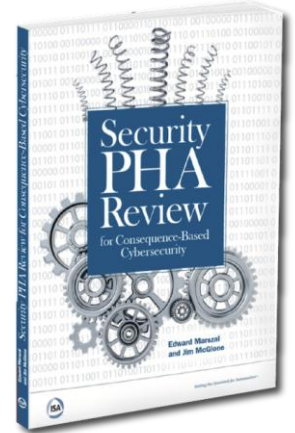
<https://gca.isa.org/blog/structuring-the-isa-iec-62443-standards>



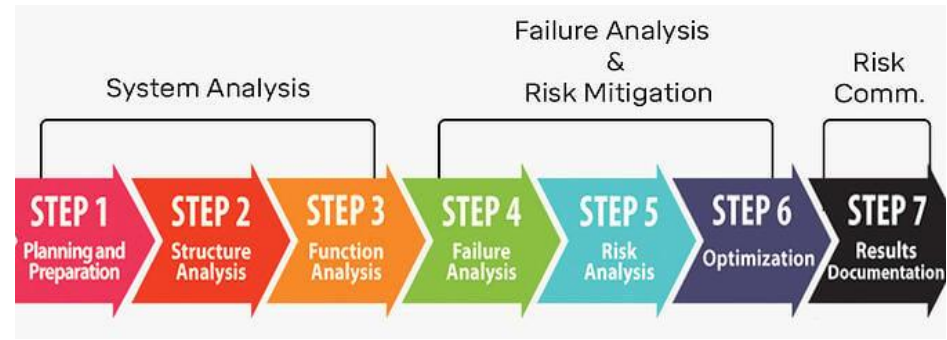
<https://www.nist.gov/image/nist-cybersecurity-framework-20>



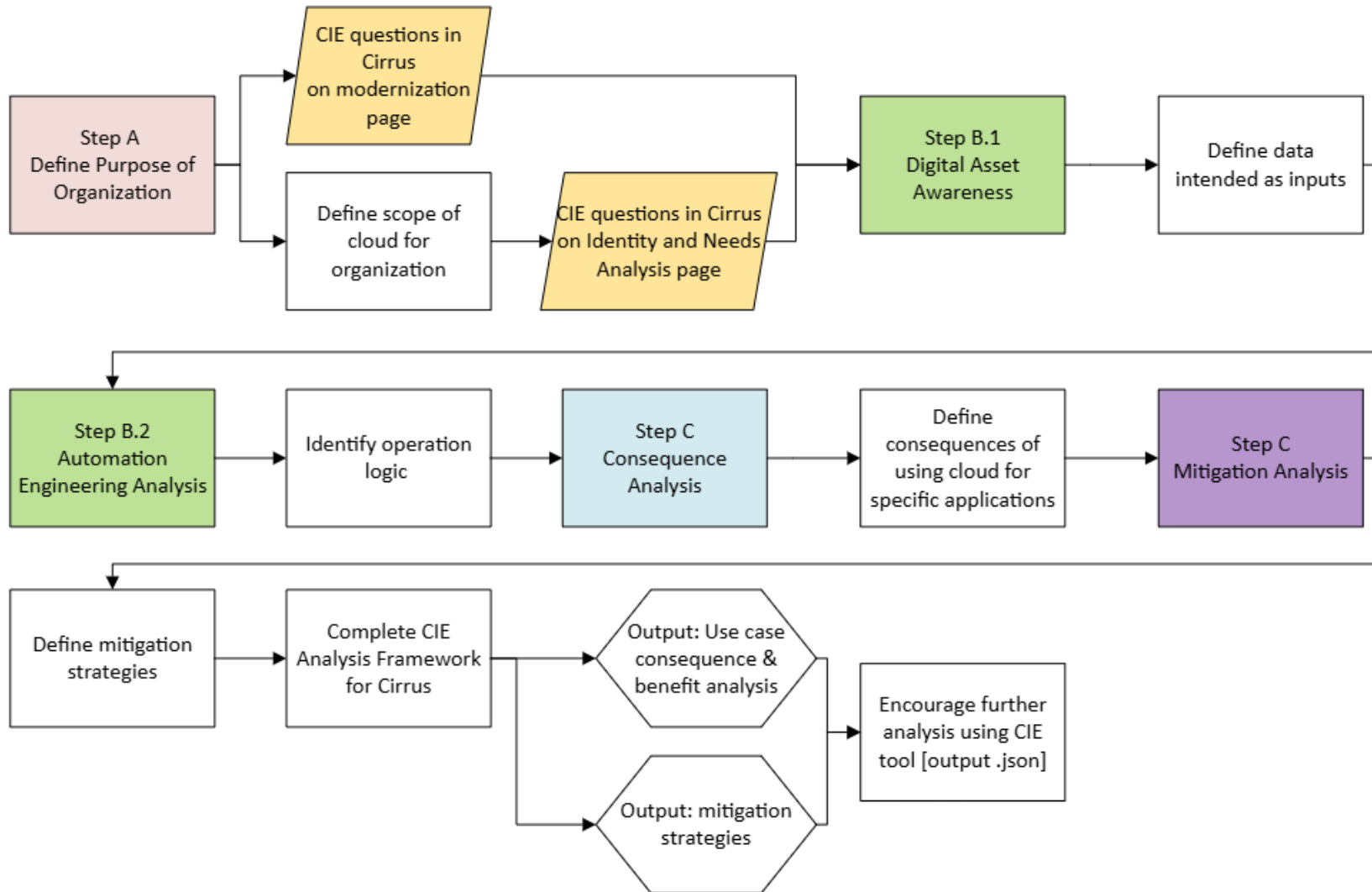
<https://incose.onlinelibrary.wiley.com/doi/epdf/10.1002/j.2334-5837.2021.00839.x>



<https://www.linkedin.com/pulse/cyber-pha-perfect-technique-ensure-your-safety-sis-kramer-mba/>



# CIE in Cirrus



# CIE Questions in Cirrus

CIE Step	CIE Question	Cirrus Step	Cirrus Question(s)
Define Purpose of Organization	Define the purpose of the X system	Identity and Needs Analysis	<ul style="list-style-type: none"> <li>• Business Model</li> <li>• Transmission &amp; Distribution</li> </ul>
Define Purpose of Organization	What parts of the design will contain X components or subcomponents?	Identity and Needs Analysis	<ul style="list-style-type: none"> <li>• Existing cloud status</li> <li>• Do you use an MSSP or MSP?</li> </ul>
Digital Asset Awareness	How are digital assets used to meet system requirements?	Modernization Strategy	<ul style="list-style-type: none"> <li>• What applications are being deployed by your organization?</li> </ul>

- This is not a full list of all CIE questions in Cirrus, just a brief demonstration of overlap
- Many of the CIE questions ask ‘how’ – Cirrus needs to know ‘what’ AND ‘how’

# Use Case Consequences & Benefits Analysis

Table 1: Example consequence table and weighting.

Criteria	None	Low	Medium	High
Area/Load Impact	Inconsequential	Loss of failure to service firm load of less than XMW	Loss of failure to service firm load between X+1 and Y MW	Loss of failure to service firm load greater than Y + 1 MW
Duration	Inconsequential	Return of all service in less than 1 day (inability to serve firm load) or supply outage for less than one week	Return of all service 1 – 5 days (inability to serve firm load) (or) supply outage for 1 week – 1 month	Return of all service >5 days (inability to serve firm load) (or) supply outage >1 month
Safety	Inconsequential	Risk onsite	Definite safety risk offsite	Loss of life potential
Cost	Inconsequential	Significant but can recover	Multiple years to recover financially	Trigger of liquidity crisis/potential bankruptcy

- Examine **interdependencies within the communication system** and establish redundancy requirements.
- Evaluate data throughput and storage needs, considering the **cost implications** of interdependency, long-term and short-term storage, redundancy, and residency.

# Risk Mitigation Strategies

- Introduce simplification by identifying essential features for the cloud deployment, exploring the possibility of reducing features to mitigate risks, and determining the most crucial aspects to mitigate High Consequence Events (HCE).
- **Phase in features gradually** with a heightened review of equipment capabilities over time, minimizing elements at risk for mission-critical functions in the initial deployment.
- Determine the minimum viable set of information to maintain operation in the event of service interruption to maintain consistent core data for analysis.
- Based on the insights gained from Secure Information Architecture and Digital Asset Management Planning (in Cirrus),
  - Data ownership guide for users to reference to address data integrity and compliance.
  - Outline cloud-handling types and offer **guidance on enhanced information protection considerations**
    - Public
    - Private
    - Hybrid
    - IaaS
    - PaaS
    - SaaS

# Cirrus User Interface Updates

The screenshot shows the Cirrus user interface home page. At the top left is the Cirrus logo and the word "IRRUS". At the top right are "ABOUT" and a user profile icon. The main heading is "Explore cloud integration and develop a strategy". Below this is a large "Welcome to" text with a cloud icon. A central "Cloud Assessment" modal is open, containing the text: "Are you interested in taking the Cirrus assessment or in viewing the assessment? Your answers will not be saved when viewing the assessment." Below this text are two buttons: "VIEW ASSESSMENT" and "TAKE ASSESSMENT". To the right of the modal, there are two columns of text: "Define your organization, key performance attributes, and risk profile" and "Cirrus runs your assessment answers through predefined models". Below this is a "Develop a Strategy" section with a cloud icon and the text "Develop a cloud strategy based on your recommendations". At the bottom are two buttons: "CLOUD ASSESSMENT" and "BEHAVIORAL ASSESSMENT".

The screenshot shows the Cirrus user interface assessment page. At the top left is the Cirrus logo and the word "IRRUS". At the top right are "ABOUT" and a user profile icon. On the left is a vertical navigation menu with 13 items: 1. Modernization Goals, 2. Key Performance Indicators, 3. Application Taxonomy and Decomposition, 4. Benefit and Consequence Analysis, 5. Preliminary Metrics, 6. Costs, 7. Develop Engineering Controls, 8. Secure Information Architecture, 9. Use Case Analysis, 10. Cost Analysis, 11. Report. The main content area is titled "Cost Questions" and contains two questions. The first question is "How often will you need to access your system/data?" with a dropdown menu set to "A mix of both" and a gauge chart showing a needle pointing to the green section. The second question is "Do you anticipate needing multi-region availability/transferability for your data?" with a dropdown menu set to "Single-region" and a gauge chart showing a needle pointing to the green section. Below each question is an "Additional Information" link. The page also includes a paragraph of text: "Implementing cost-effective strategies and maintaining a budget-conscious approach will pave the way for a smooth transition to the cloud. Questions on this page have options ranging from low to high cost relative to the other options within the questions. The aim is to give you a ballpark of what to expect without being tied down to hard numbers."

# Publication Updates and Next Meeting

- Next meeting
  - June 12<sup>th</sup>?
  - June 19<sup>th</sup>?
- Final meeting
  - September 18<sup>th</sup>?

Artifact Type	Publication, Report, Presentation, Paper, Conference, etc. Title	Publication Date	External Publication Link (Including OSTI)
Conference Papers	Evaluation and Use Cases in Cloud Implementation for Future Electric Grid Technologies	July 21, 2024	<a href="https://ieeexplore.ieee.org/document/10688615">https://ieeexplore.ieee.org/document/10688615</a>
Technical Reports	Lessons Learned for Responsible Use of Cloud in the Cirrus Project, Following the CrowdStrike Outage Event	October 11, 2024	<a href="https://www.osti.gov/biblio/2482012">https://www.osti.gov/biblio/2482012</a>
Technical Reports	Enhancing Cloud Cybersecurity: Prescriptive Controls for Operational Technology	October 22, 2024	
Conference Papers	Consequence Based Framework for Deployment of Cloud Solutions in the Digital Energy Transition	January 21, 2025	<a href="https://ieeexplore.ieee.org/document/10887455">https://ieeexplore.ieee.org/document/10887455</a> <a href="https://www.osti.gov/biblio/2510493">https://www.osti.gov/biblio/2510493</a>
Conference Papers	Improving Cybersecurity and Resilience through Cloud Technology Implementation	February 4, 2025	



# Idaho National Laboratory

*Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.*

# IAB & COP Charter

- **Publication**

- The IAB members have the right to publicize the fact of their participation in the IAB. They have the right to disseminate work products from the projects, provided that the work products have been cleared for release by the laboratory and DOE GDO.

- **Responsibilities**

- The IAB members are responsible to attend bi-annually virtual meetings (once every six months) to provide feedback as requested of them and to review the work products (if any). IAB members are also responsible to not disclose their own company's proprietary or other sensitive information during IAB meetings or in their written feedback. The Community of Practice will meet online monthly. Attendance is encouraged but not required, and will be intended to guide the future of this work in cloud implementation.

- **Meetings**

- The project team will host bi-annually virtual IAB meetings to solicit the feedback. The IAB members are also encouraged to join the annual in-person continuation review meeting.

- **Commitment**

- The project team estimates that IAB members are not expected to spend more than 2 hours on IAB work every month. The actual time may vary from month to month.

- **Term of Membership**

- The IAB will exist for the duration of the project, which is scheduled to end September 2024. The minimum expected term of IAB membership is one (1) year.

# Use Case Descriptions – general details about implementation factors to decide cloud benefits and purpose

- **Security and Compliance**

- Cloud-based cybersecurity solutions can provide robust protection against cyberattacks, data breaches, and unauthorized access to sensitive information. Cloud providers offer advanced security measures, including encryption, firewalls, and intrusion detection systems, to safeguard utility data and comply with industry regulations.
  - Increased penetration of renewable energy sources.
  - Improved grid flexibility and resilience.
  - Reduced reliance on traditional fossil fuel-based generation.

- **Reliability and Planning**

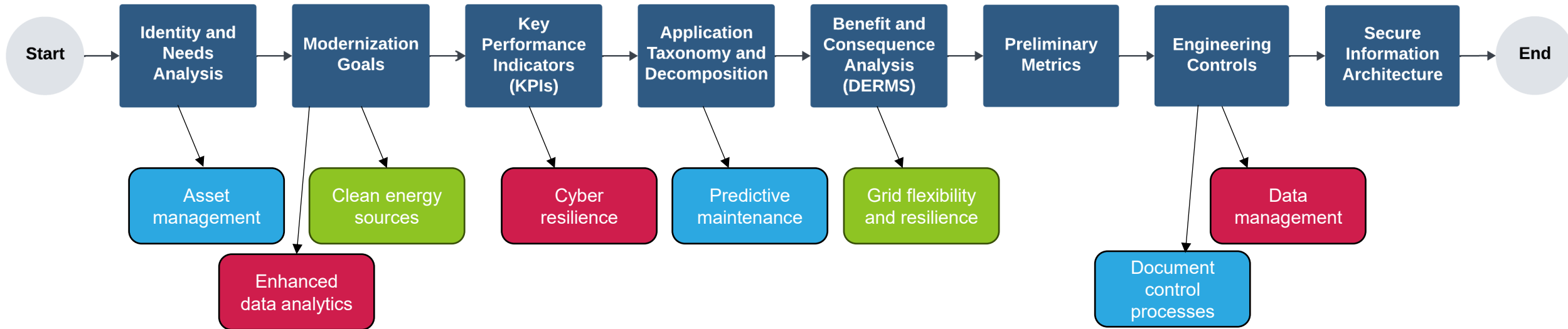
- Reliability and planning models are crucial for utility distribution systems to ensure the efficient and reliable operation of power grids. Reliability models focus on analyzing the performance and dependability of the distribution system by assessing the probability of component failures, identifying potential causes, and estimating their impact on the overall system. Utilities use reliability models in the following ways:
  - Equipment maintenance and asset management to share data between entities for better analytics (improve size of the data pool for advanced functions that do not work with small silos).
  - Reliability and planning model.
  - Engineering drawing management.

- **Grid Management and Optimization**

- Cloud-based solutions can provide real-time visibility into grid operations, enabling utilities to optimize power distribution, manage demand fluctuations, and prevent outages. Cloud-powered analytics can analyze vast amounts of data from sensors and smart meters to identify patterns, predict potential disruptions, and implement proactive measures. Benefits associated with grid management and optimization include the following:
  - Advanced Distribution Management Systems
  - Smart Metering and Enhanced Data Analytics
  - Distributed Energy Resource Management System
  - Equitable Technology Access and Cyber Resilience
  - Data Management and Planning Tools

# Use Case – Intention for assessment taker

- How do we use existing information for analysis?
- Do we need to expand the assessment for more effective analysis?



# Use Case – Participant and Data Relation

How do we associate observed information with actionable items?

## 1. Technical vs. visual output

- Suggested actions based on category (previous slide)
- Static information based on assigned use case
- etc

## 2. Pros and Cons – thoughts?

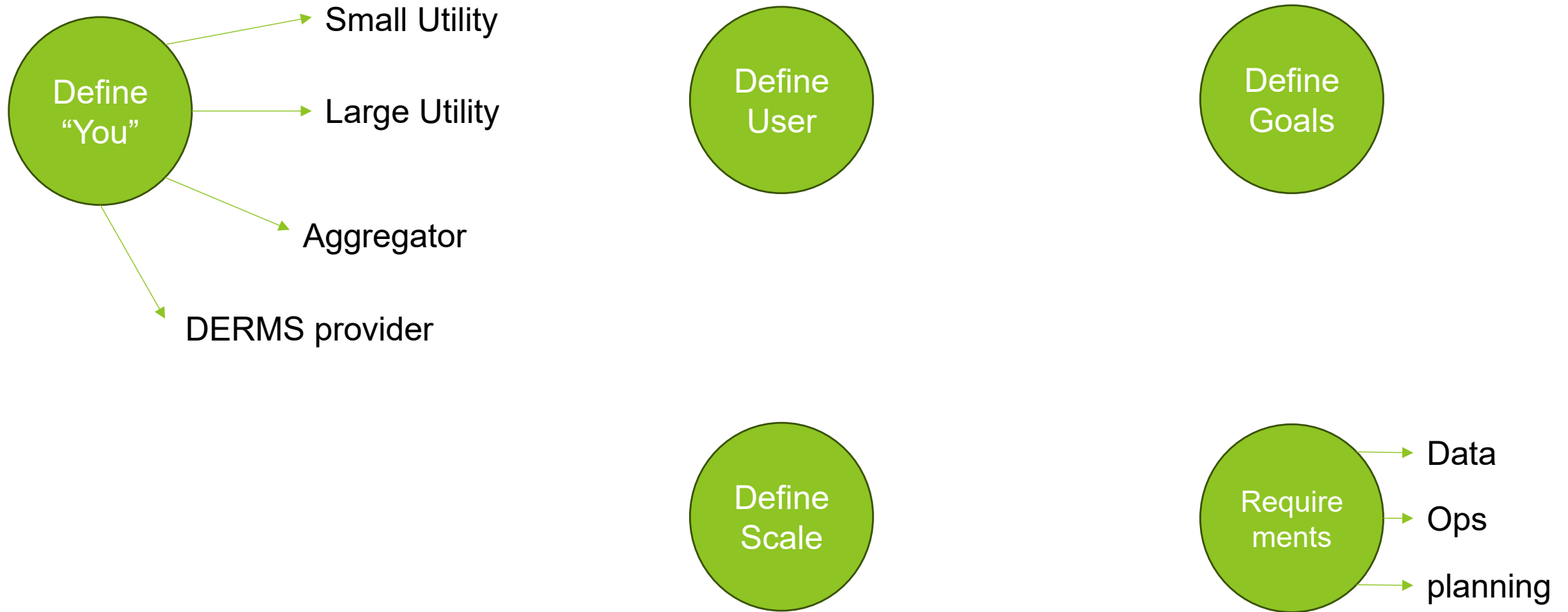
## 3. Characteristics associated with cost

- Evaluation of utility (function vs. purpose)
- Identify significant annual costs
  - Business expenses (stakeholder engagement)
  - Alternative energy sources
  - Physical safety
  - Cyber safety
  - Systems and Services
    - Operational maintenance

# Stakeholders

- Small/medium utilities building modernized infrastructure
  - Overall digital infrastructure shift
  - Board report
- Utility Staff Planning Deployment of Advanced Applications
  - Determine if cloud is the right choice
  - Cost targets
  - Initial planning framework
  - Find the right questions to ask the third party/vendor
- Decision makers
  - NERC CIP? Regulated? Non Regulated?
- Third Party integrators
  - DERMS Software, ADMS provider, start up/new applications
  - Cloud or not cloud and what requirements will there be

# Example Types of Questions in the Decision Support Framework



# Consequence (its good and bad)



**What is the purpose of the proposed system**

How does it support the org  
What sys processes exist for this function  
What sys processes if they fail or operate incorrectly, will cause the purpose to fail



**What are the mission critical functions it must perform**

What aspects of the CONOPS enable the functions  
What needs does it address in the system and how does it do that?



**What short term outcome is needed from this application (metrics for success)**

Net zero targets  
Cost reduction  
Improve security



**What Consequences from failure or unexpected operations**

Impact to delivery, safety, security, the environment, property, financials, or corporate reputation  
What happens if multiple consequences at once

# Plan for engagements

- 3 x IAB Meeting – 1 year (inc kick off)
  - Online (Feb 28 – potentially in person @ dtech?)
  - 1 in person
  - Poll for common in person events
- Monthly COP Meetings (No 1. Dec 6 or 7)
  - Online Teams Forum
  - Review progress
  - General discussion on cloud applications
  - Beta test
- Publications
  - Roadmap for review
- Resilience Week Meeting (Nov 27 – 29 in DC)

# Outreach Events

- Distributech
  - Planned workshop
- IEEE PES GM (July 2024)
  - Paper/Panel
- Gridwise Alliance (Dec)
  - Attendance
- RSA Submitted (May 2024)
  - Panel
- RE+ Submitted
  - Workshop
- Clean Energy Cyber con? (Feb)
- SANS ICS 2024 (Orlando?)
- Trade Events
  - APPA National Meeting (June)
  - ACP National Meeting (May 6 – 9)
  - EEI National Meeting (June)
- EV Charging Expo and Summit?
- Cloud Company Events
  - AWS Summit 2024 (June 26 + 27)
  - Google Cloud Next 2024 (Aug 29 – 31 LV)
- ESIG Workshops

# Feedback & Homework

- Guiding the features and decision support?
- Joining the COP
- In person Event choice?

## 8. CIE Principles (Website/tool will have a guide to each of these and how to work through it)

PRINCIPLE	KEY QUESTION
<b>Consequence-Focused Design</b>	How do I understand what critical functions my system must <u>ensure</u> and the undesired consequences it must <u>prevent</u> ?
<b>Engineered Controls</b>	How do I implement controls to reduce avenues for attack or the damage which could result?
<b>Secure Information Architecture</b>	How do I prevent undesired manipulation of important data?
<b>Design Simplification</b>	How do I determine what features of my system are not absolutely necessary?
<b>Layered Defenses</b>	How do I create the best compilation of system defenses?
<b>Active Defense</b>	How do I proactively prepare to defend my system from any threat?
<b>Interdependency Evaluation</b>	How do I understand where my system can impact others or be impacted by others?
<b>Digital Asset Awareness</b>	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?
<b>Cyber-Secure Supply Chain Controls</b>	How do I ensure my providers deliver the security we need?
<b>Planned Resilience</b>	How do I turn “what ifs” into “even ifs”?
<b>Engineering Information Control</b>	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
<b>Cybersecurity Culture</b>	How do I ensure that everyone performs their role aligned with our security goals?