



Resiliency Summit

Participant Handbook



July 2024



Ask a Question. Get an Answer.
Scan to access Resiliency resources and
industry discussion on Nuclear Community.

The Resiliency Summit will facilitate understanding of the principles document and its application. INPO, industry and external experts will facilitate sessions to present a case for change, provide additional detail on the principles, and share information on implementation. Attendees will leave the summit equipped to align their organizations on the resiliency principles and lead implementation.

At the conclusion of the Summit, attendees will be equipped to:

- **Communicate the case for change for resiliency.**
- **Explain the resiliency definition, model and principles.**
- **Apply the resiliency principles to a variety of threats, recognizing strengths and vulnerabilities in their organization.**
- **Identify the next steps for implementing the resiliency principles in their organizations.**



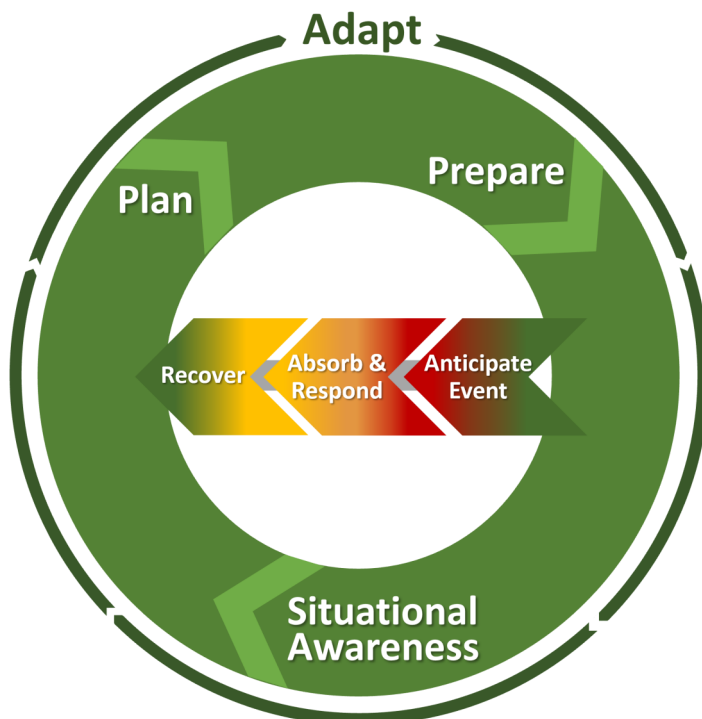
Notes *from the* **Executive Message**

This image shows a single sheet of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page. There are approximately 20 lines visible. The paper has a slight shadow on the right side, suggesting it's resting on a surface.



Notes *from* Resilient Critical Infrastructure

The Resiliency Principles



- Develop and maintain **Plans** to improve physical robustness to absorb and organizational readiness to respond to credible external threats.
- **Prepare** for external events by increasing the physical capability to absorb impacts and the organizational readiness to respond.
- Maintain **Situational Awareness** of real-time information and future projections to adapt plans and preparations.
- **Anticipate** and mitigate impending and emerging challenges to continuously position the plant and organization for the best outcomes.
- **Absorb and Respond** to event impacts to maintain continuity of operations without challenging nuclear safety.
- **Recover** from external events by restoring stable plant conditions and operating margins and re-establishing readiness to respond.
- **Adapt** plans and preparations to strengthen the capability to absorb and respond to external threats.

Action Planning *for* **Resilient Critical Infrastructure**



Identify 3 insights or action items from this session:

1

2

3



Analyzing *the Principles* — SWOB

Threat Categories	Strengths —	Weaknesses —	Opportunities —	Barriers —
	What do we currently do well? What is our strongest advantage?	Which principles need the most improvement? What are other industries doing that we aren't?	How can we apply new thinking or learn from others? What trends or initiatives can we leverage?	What factors could hinder our progress? What are the communications or organization pitfalls?
Cyber				
Physical				
Natural				
Indirect				

Action Planning *for* SWOB Analysis



What actions can I take to support the resiliency threat categories based on the strengths, weaknesses, barriers and opportunities identified?

Cyber



Physical



Natural



Indirect



Notes *from the* Keynote

Keynote *Key Takeaways*

Identify 3 insights or action ideas from this session:

1

2

3



Applying *the* Principles — Case Studies

Case Study Summary: Wildfire in Paradise

A wildfire named the "Camp Fire" was reported near Paradise in the early morning. One hour later, the Butte County Sheriff's Office ordered an evacuation. However, many residents never received an evacuation warning, while others chose not to leave because the warnings did not convey the urgency of the situation. Other locations were also issued evacuation orders or warnings, and emergency shelters were established.

The Camp Fire was caused by a faulty transmission line that ignited dry vegetation after six years of drought. High winds of up to 50 miles per hour drove the fire quickly and much of the town of Paradise was destroyed in less than 6 hours. A total of 85 people died, tens of thousands were displaced, and 18,804 buildings were destroyed. Only 5 percent of buildings in the town remained without serious damage after the fire.

Case Study: Road Washout on County Road 114

During June 2012, record amounts of rainfall in the Duluth area of northeastern Minnesota brought about a 500-year flood event. Swollen rivers and flash floods washed away or damaged several bridges and rendered large sections of roadway impassable, including a primary road to the Fond du Lac (FDL) Reservation that was essential for access to homes and emergency services. The FDL tribal council operates social services, tribal housing, a tribal police force, a natural resource building, a gas station, three community centers, and a private health clinic and pharmacy. The tribe also owns two casinos. The 4,184 residents of the FDL Reservation were isolated until the road was fully restored to service 16 months later.

Case Study: Supply Chain Disruption at Toyota

When production came to a screeching halt at 14 Toyota assembly plants in September 2023, the automobile industry took notice. A fault in the parts order management system meant production could no longer be maintained. It was a surprising setback given that Toyota is renowned for its "just-in-time" (JIT) principle, stemming from the Toyota Production System, initiated by Kiichiro Toyoda. The success of the JIT approach hinges on the timely delivery of all goods, components or materials, which hadn't been the case since the outbreak of the pandemic. In this instance, the parts management system fault delayed the delivery of chips from Taiwan. This created bottlenecks that led to production stoppages. Toyota Motor Manufacturing in Kentucky recovered more quickly than other automakers but is still trying to improve supply chain resiliency.

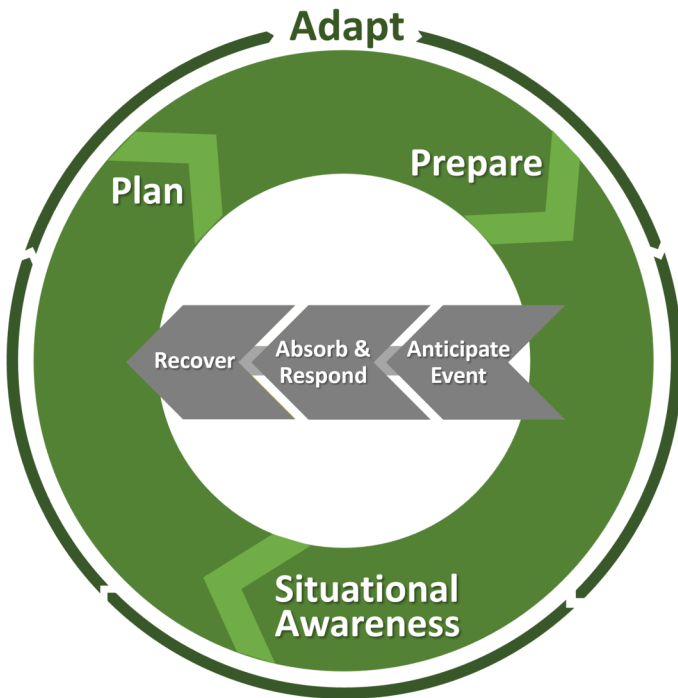
Case Study: Cyber Attack in Fremont County

At 2:00 am, August 16, 2022, the entire Fremont County, Colorado internal communication network failed because of a ransomware cyberattack. County officials discovered the county's systems had been hacked, using social engineering and deceptive messages to trick users into granting access to their system. Communication connectivity to — and between — county departments was down. County business came to a halt. The state's radio system remained uncompromised, and most emergency response agencies were still in operation. But across the county, other departments — including the transportation department, Department of Public Health, sheriff's office, and the Fremont County Administration Building — were locked out and unable to serve the county's 50,000 residents. The administration building houses many services including the county assessor, treasurer, coroner, veterans' services, and planning and zoning. As the county manager put it, "it was as if everything had just been unplugged."



Applying *the* Principles — Case Studies

My Assigned Case Study: _____



Recommended Principle: _____

Why? _____

How can this principle best be leveraged? _____

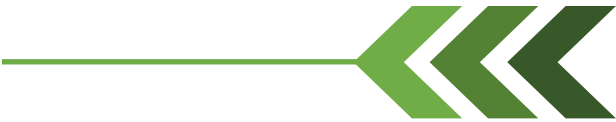
Recommended Principle: _____

Why? _____

How can this principle best be leveraged? _____



Action Planning *for* Case Studies



Identify insights or ideas you might apply from each case study:

Wildfire



Road Washout



Supply Chain



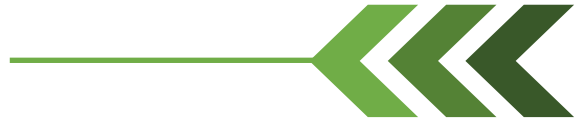
Cyber Attack



Welcome to...

Resiliency Summit Day 2

Key Takeaways *from* Day 1

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



Notes *from the* **Principles Implementation Panel**

Action Planning *for* **Principles Implementation**



Identify 3 insights or action items from this session:

1

2

3



Building *a* Resiliency Strategy

Activity Scenario:

Experts are predicting the next pandemic will occur in the next 3-5 years. They think it will be less impactful to adults but much riskier for children. It is anticipated that households with minor children would need to isolate completely. Also, some nations that provide key supplies have pledged to more quickly close their borders and limit trade if another pandemic occurs, which will specifically impact the availability of computer chips for multiple applications.

How would you strengthen your threat-specific strategy for each principle?

My Assigned Principle: _____

Notes *from* Group Discussion:

Plan	
Prepare	
Situational Awareness	
Anticipate	
Absorb & Respond	
Recover	
Adapt	

Action Planning *~* Resiliency Strategy



Identify 3 insights or action items from this session:

1

2

3





Notes *from* Next Steps

Next Steps *and* Action Planning



Identify 3-5 goal ideas to begin change management and implementation of the resiliency principles at your organization.

1

Implementation : _____

Change Mgmt : _____

2

Implementation : _____

Change Mgmt : _____

3

Implementation : _____

Change Mgmt : _____

4

Implementation : _____

Change Mgmt : _____

5

Implementation : _____

Change Mgmt : _____

Next Steps *and* Action Planning



Using the three goals identified on the previous page, begin planning your highest priority actions to support those goals.

GOAL

Highest Priority Actions

1.

2.

3.

4.

GOAL

Highest Priority Actions

1.

2.

3.

4.

GOAL

Highest Priority Actions

1.

2.

3.

4.

17

18