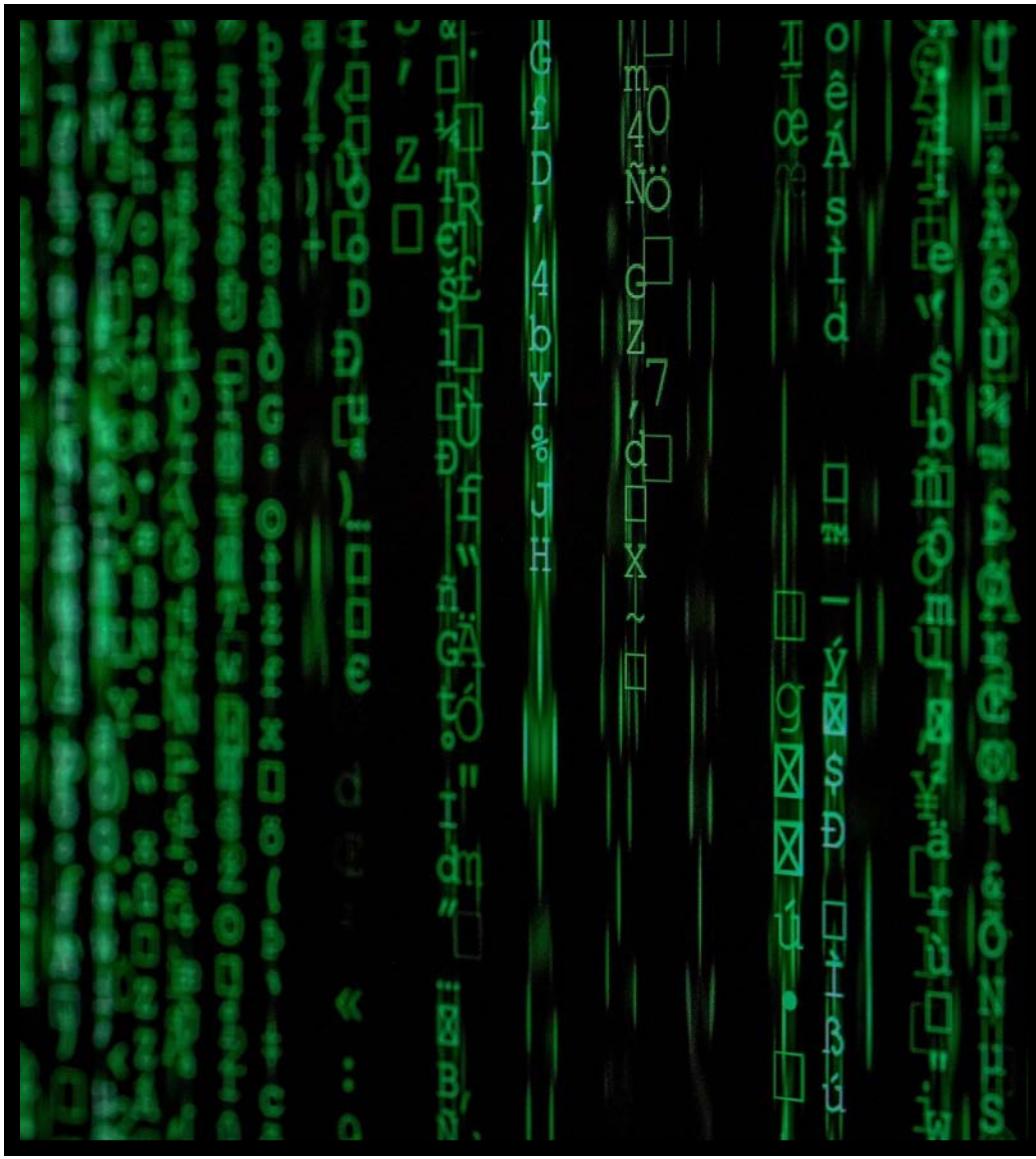
Operations Track

Demonstrating Privacy ROI: Securing Leadership Buy-In and Building Public Trust



Demonstrating Privacy ROI:

Securing Leadership Buy-in and Building Public Trust.

Portions of this presentation were developed with the assistance of artificial intelligence. All content has been reviewed, edited, and approved by the presenters.

Introducing Our Speakers

Shanna Durrant
Privacy Officer
Utah Department of Public Safety

Jodi Shegrud
Director of Privacy
Utah Department of Government Operations

Our Agenda

Moving from Compliance to Strategy

The Business Case

The Leadership Panel

The Deliverable: A data-backed script to secure the resources and staff you need.

Privacy Friction Myths

The Compliance Stigma

95% 'System Stop' risk when privacy is treated as a late-stage roadblock.

The Visibility Gap

75% lag time in privacy reviews due to shadow IT and late involvement.

The Ownership Myth

43% of agencies do not prioritize privacy, making it 'everyone's job, no one's responsibility.'

Sharpening the Axe

Enhancing efficiency through proactive data management.

- Clear Stewardship

  Minimize internal confusion, duplicate decisions, and blurry boundaries by defining clear data ownership and responsibilities.

- Defensive Retention

  administrative record-keeping burdens through careful deletion of unnecessary data.

Transitioning from reactive, informal data storage to intentional, mature data management practices.

Risk Prevention

Reactive Protection vs. Proactive Governance

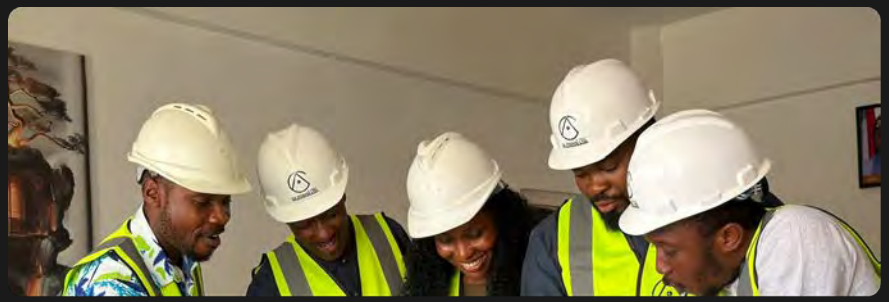
Focus: Mitigating breaches and disasters.

Approach: Reacting to failures.

Data Practices: Ad-hoc adjustments after breaches.

Third-Party Control: Minimal oversight with reactive enforcement.

Outcome: Corrective measures and damage mitigation.



Focus: Defensible data use and vendor oversight.

Approach: Preventing failures.

Data Practices: Legally, operationally, and publicly justifiable.

Third-Party Control: Contracts aligned with agency requirements.

Outcome: Mitigated risks before systems are built.

Speed with Safety: Privacy as an Innovation Enabler

Sovereign Foundations

- Secure data standards enable confident AI deployment.

The Result

- Faster public issue resolution and 24/7 automated support with zero data leaks.

"Privacy is not a brake; it is the guardrail."

Privacy as a Community Collaborator

Open Data Catalogs

Data Education & Collaborative Community Events

The Results

- Proactive and enhanced community engagement
- More robust datasets and public feedback
- Increased citizen support for adoption of technology

"Privacy is a necessary precursor for innovation."

Building Public Trust

Data Stewardship

- 61% of U.S. citizens prioritize secure data handling.
- 41% trust the government to manage it.
- 54% state that clear transparency regarding data use directly influences their comfort level with utilizing digital government services.

"An organization's approach to privacy impacts more than compliance. Investment in privacy drives business value across sales, security, operations, and most importantly, trust."

Key Takeaways

Operational Efficiency

Privacy, when strategically implemented, contributes to smoother operations.

Risk Mitigation

Privacy practices help in reducing potential risks.

Responsible Innovation

Privacy enables innovation that is both ethical and forward-thinking.

Public Trust

Building and maintaining public trust through strong privacy measures.

It's time to move beyond compliance and leverage privacy as a strategic asset.

Introducing Our Panelists

Marilee Richins
Deputy Commissioner
Department of Government Operations

Brian McKenzie
Davis County Clerk
Davis County

Betsy Haws
Senior City Attorney
Salt Lake City Corporation

Thank You for Joining Us!

Jodi Shegrud
jshegrud@utah.gov

Shanna Durrant
shannadurrant@utah.gov

Scan for Handouts

"Privacy is the foundation of digital trust."

Operations Track

Operationalizing Utah's New Privacy Maturity Models

Shane Paul
Privacy Training Director
Utah Office of Data Privacy

Micah Vorwaller
Deputy Chief Privacy Officer
Utah Office of Data Privacy

Shane Paul Presentation

Operations Track

From Panic to Plan: Taming Your Biggest Privacy Risks

Jodi Shegrud
Director of Privacy
Utah Department of Government Operations

Stephen Cannon
Chief Information Security Officer
City of Orem


FROM PANIC
TO PLAN
Taming Your Biggest Privacy
Risks

INTRODUCTION

Utah Privacy Summit 2026

Jodi Shegrud

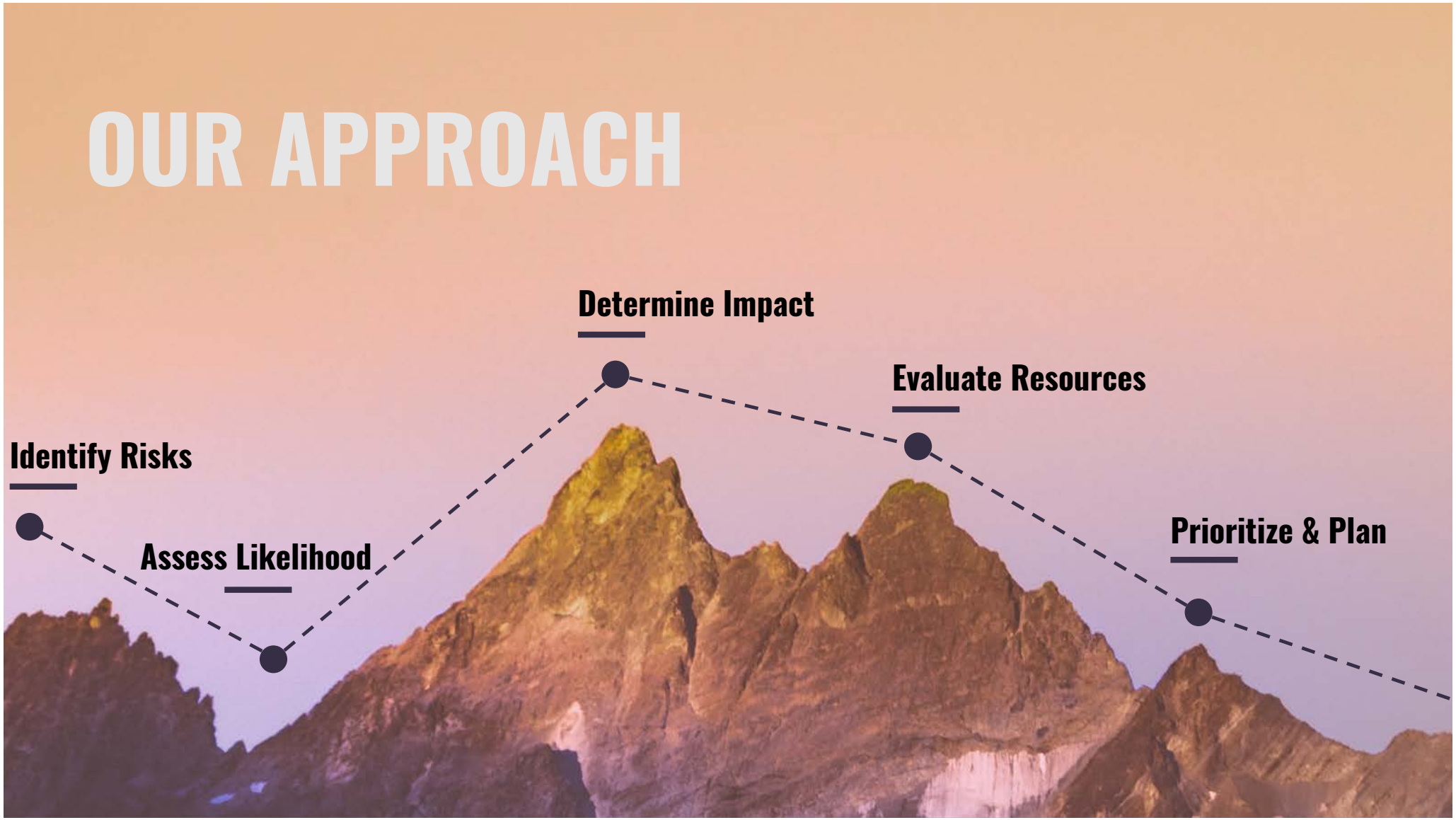
Director of Privacy
Utah Department of Government Operations

Stephen Cannon

Information Security Officer
Orem City


THE REALITY
Every Organization has gaps
You can’t do everything at once.
The goal isn’t immediate perfection. The goal is better.

OUR APPROACH




You are here.
Accept that everyone is non-compliant.
Accept that you can't do everything at the same time.
Where you want to be.
Defensible priorities
Focused risk reduction
A realistic plan for what comes next
#1 - START WHERE YOU ARE

#2 - KNOW THE RULES

1 General Privacy and Records

Government Data Privacy Act
GRAMA
etc.

2 Industry / Sector Regulation

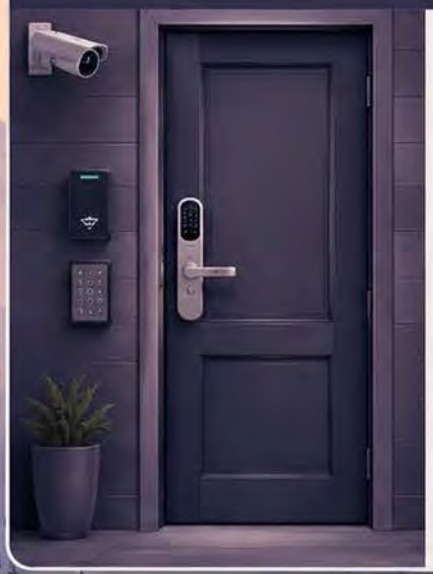
Criminal Justice Information
Health Data
etc.

3 Local/Org Obligations

Contracts
Policies
etc.

Security vs. Privacy

SECURITY

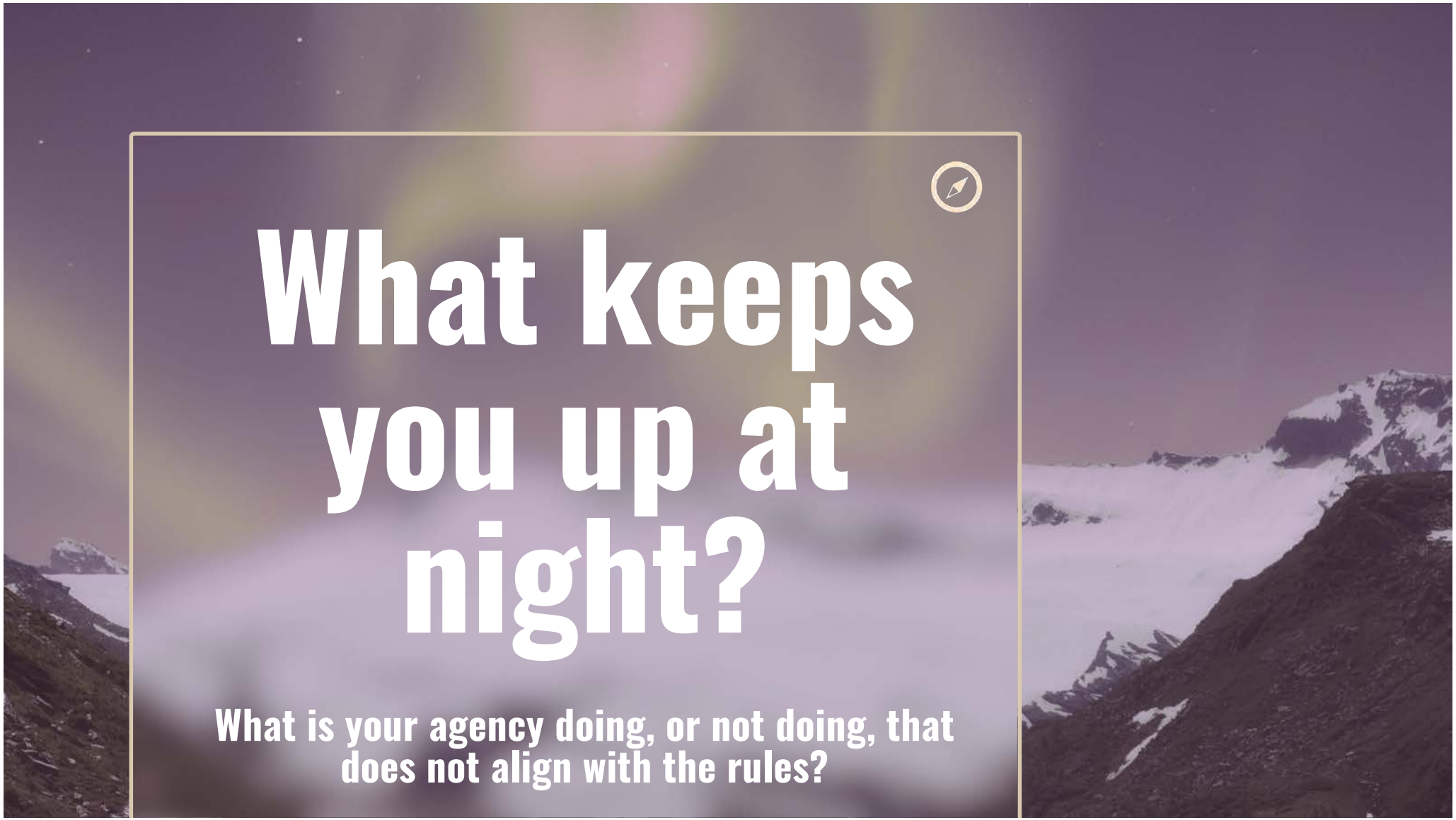


Security is concerned with the door — the locks, badges, cameras, passwords, and whether unauthorized people can get in.

Is the door locked? Who has a key? Do we know if someone forced it open?

PRIVACY

Privacy is concerned with what is behind the door — what personal data was collected, why it is kept, who can use it, how long it stays, and what happens if it is exposed or misused.


What keeps you up at night?
What is your agency doing, or not doing, that does not align with the rules?

LIKELIHOOD

HOW PROBABLE IS THE EVENT?

CONTROLS

The effectiveness of existing safeguards in preventing risk materialization.

EXTERNAL PRESSURES

Market forces, regulatory shifts, and economic conditions.

CULTURE

Organizational values and mindset regarding safety and compliance.

COMPLEXITY

The intricacies of systems and processes that may obscure vulnerabilities.

CONTROLS: YOUR RISK TOOLKIT

How "Real" is the Guardrail?

ADMINISTRATIVE

The Rules: Policies, charters, governance documents, and assigned authority.

OPERATIONAL

The How-To: Procedures, forms, checklists, and manual workflows.

TECHNICAL

The Enforcers: System limits, automated routing, and audit logs.

Internal Conditions

CULTURE: THE HUMAN FACTOR

Workaround-heavy environments where teams avoid official processes. Culture carries as much weight as policy.

Red Flag: "Shadow processes" where staff create informal data handling methods.

COMPLEXITY: THE MULTIPLIER

Fragmented systems with multiple manual touchpoints. Each manual hand-off is a point of failure.

Risk: Routine control failure in environments with manual extraction and uploads.

Likelihood Impact: Internal Conditions

LOW RISK	MIXED	HIGH RISK
Standardized & Automated	Inconsistent Enforcement	"Almost Certain" Failure
Privacy is embedded. Minimal manual intervention. Leadership models standards.	Rules followed when convenient. Shortcuts taken when busy. Mixed budget support.	Open resistance. Privacy seen as a speed bump. Fragmented, manual systems.

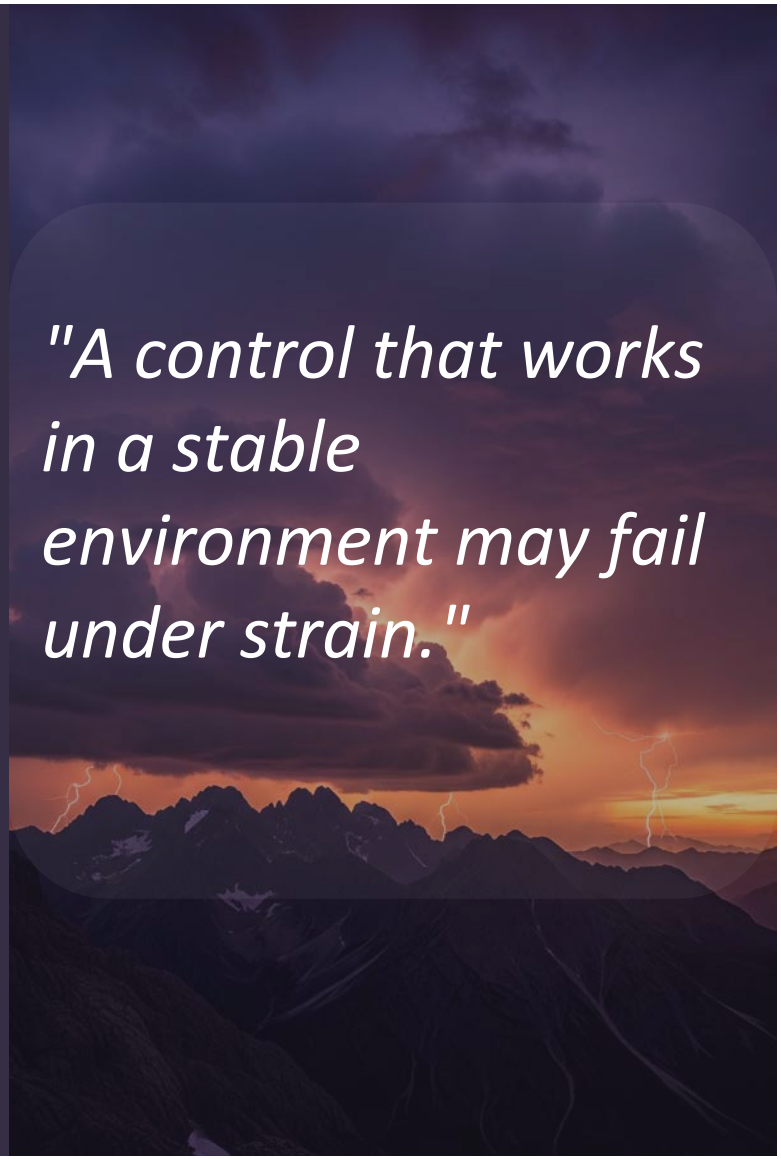
EXTERNAL CONDITIONS

UNFAVORABLE CONDITIONS

Pending regulations or "state-of-the-art" tech increasing exposure.

STABLE ENVIRONMENT

Mature vendors, well-understood tech, and static legal requirements.



DETERMINE THE IMPACT

- Context
- Scale
- Consequences
  - Recovery?
  - Effects (Reputational / Strategic)

Where risk becomes real

What actually happens if this goes wrong?

IMPACT

Key Considerations

1 Data Sensitivity

What are the data elements and the context?
Are we dealing with Protected Class?

2 Scale

How many people would be impacted?
How broadly?

3 Consequences

Could people be harmed if the event occurs? (Physically, Financially Emotionally)

4 Recovery

How long and how expensive would it be to fix this?

5 Reputational & Strategic Effects

Would an event undermine our credibility or strategic goals?

EXAMPLE: IMPACT IN CONTEXT

Where risk becomes real

What actually happens if this goes wrong?

DETERMINE RESOURCES

ADMINISTRATIVE

The Rules: Policies, charters, governance documents, and assigned authority.

OPERATIONAL

The How-To: Procedures, forms, checklists, and manual workflows.

TECHNICAL

The Enforcers: System limits, automated routing, and audit logs.

Prioritizing: Risk Score + Resources + Judgment

- Risk Score

  Assess the potential impact and likelihood of risks.

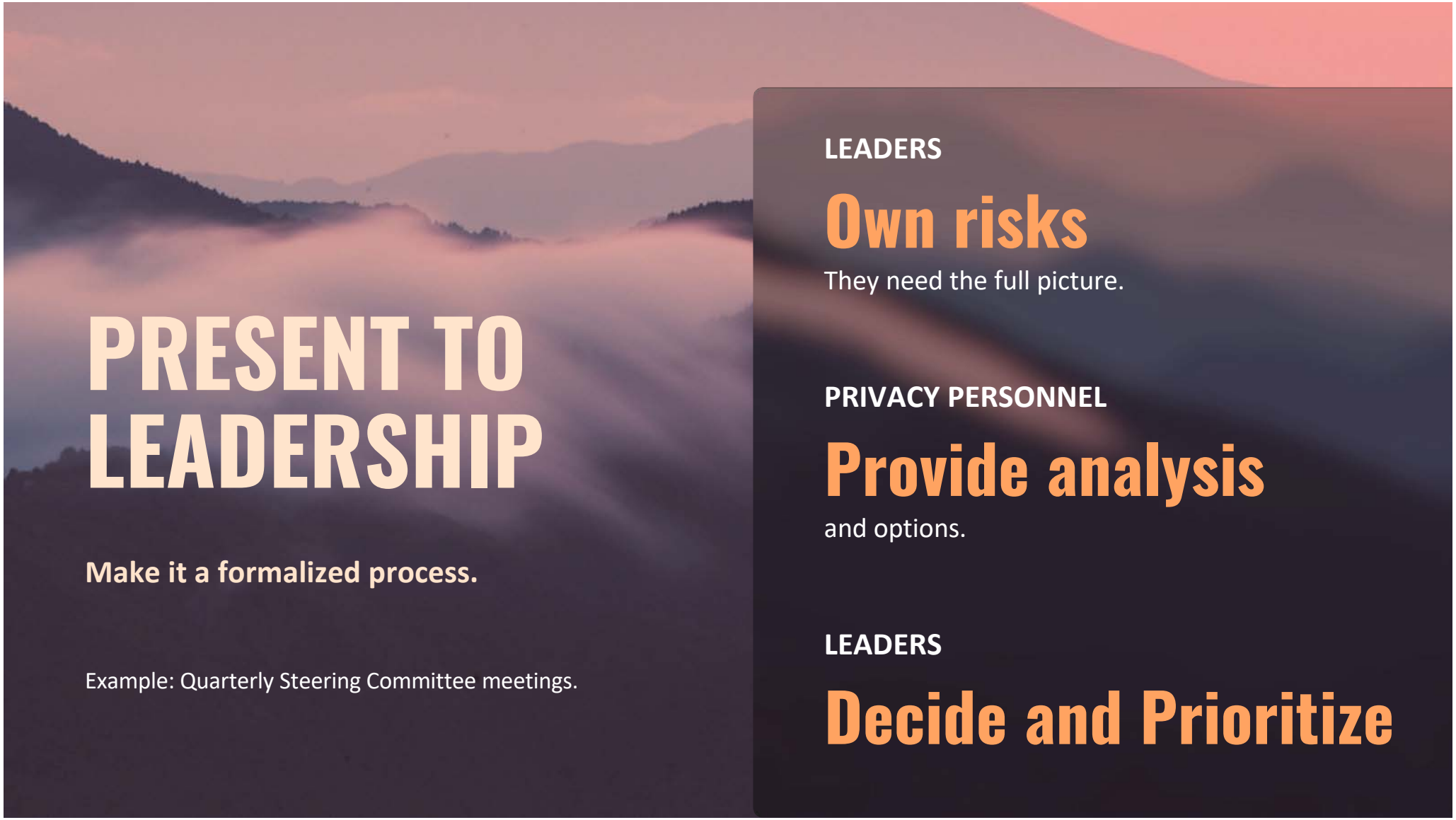
- Resources

  Evaluate the available resources (time, budget, personnel).

- Judgment

  Apply expert knowledge and strategic insights to decision-making.

Prioritize work that reduces the most risk with the resources you have.


PRESENT TO LEADERSHIP
Make it a formalized process.
Example: Quarterly Steering Committee meetings.
LEADERS
Own risks
They need the full picture.
PRIVACY PERSONNEL
Provide analysis
and options.
LEADERS
Decide and Prioritize

CLOSE

PROGRESS OVER PERFECTION

Don’t let perfect be the enemy of better.

Privacy is an iterative process.

You are not trying to get it PERFECT, you’re trying to get it BETTER.

Thanks for listening!

Thank You for Joining Us

Stephen Cannon
sccannon@orem.gov

Jodi Shegrud
jshegrud@utah.gov

Scan for Handouts

"Privacy is the foundation of digital trust."