

Maturing Your Organization's Risk & Resiliency Program

PRESENTATION

Governance, Risk Management & Compliance Insight

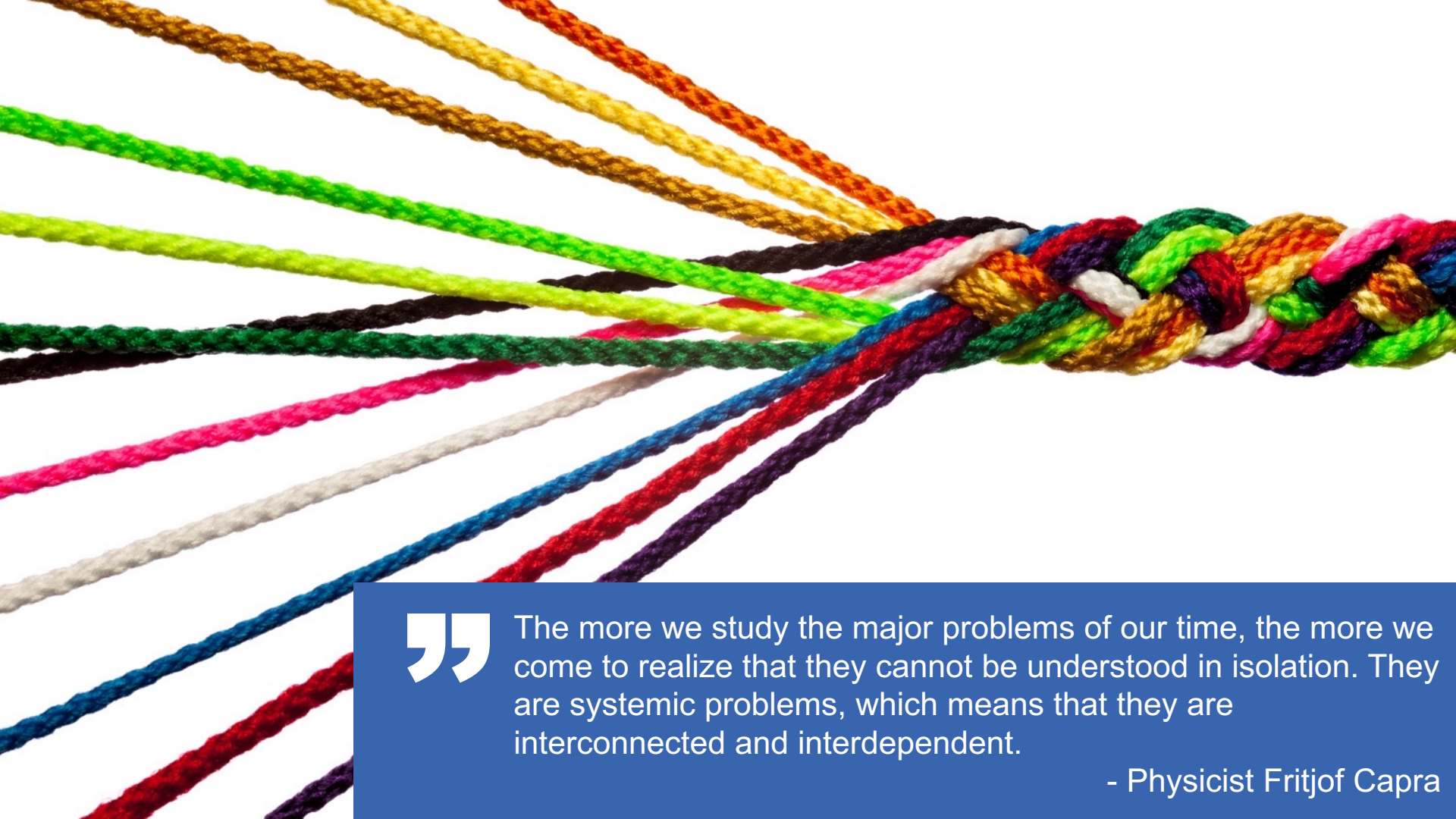
Lessons learned from 2020 and 2021



Navigating Chaos

What Have We Learned from 2020 and 2021?

- These lessons showed us:
 - ✓ Interconnected risk.
 - ✓ Objectives became dynamic.
 - ✓ Disruption.
 - ✓ Dependency on others.
 - ✓ Dynamic and agile business.
 - ✓ Values were defined and tested.
- The past two years have taught organizations that to be resilient requires a 360° view of objectives, risk, processes, and services within the organization and the extended enterprise.

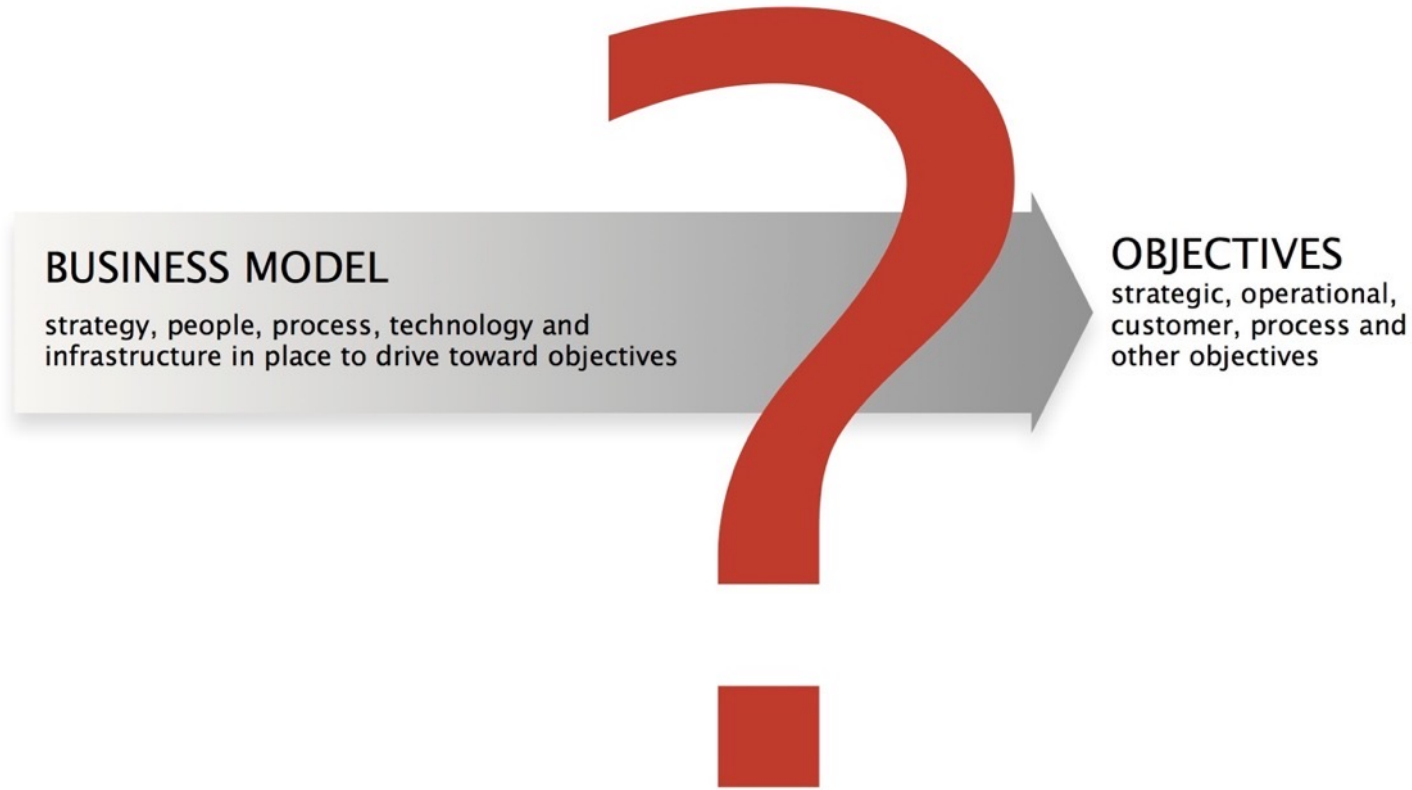


”

The more we study the major problems of our time, the more we come to realize that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent.

- Physicist Fritjof Capra

UNCERTAINTY



Inevitability of Failure: Manual & Non-Integrated Processes





The ORGANIZATION Has to be Able to See . . .

The Tree. The individual risk

The Forest. The interconnectedness of risks and objectives

Agility: New Directions in Risk & Resilience Management

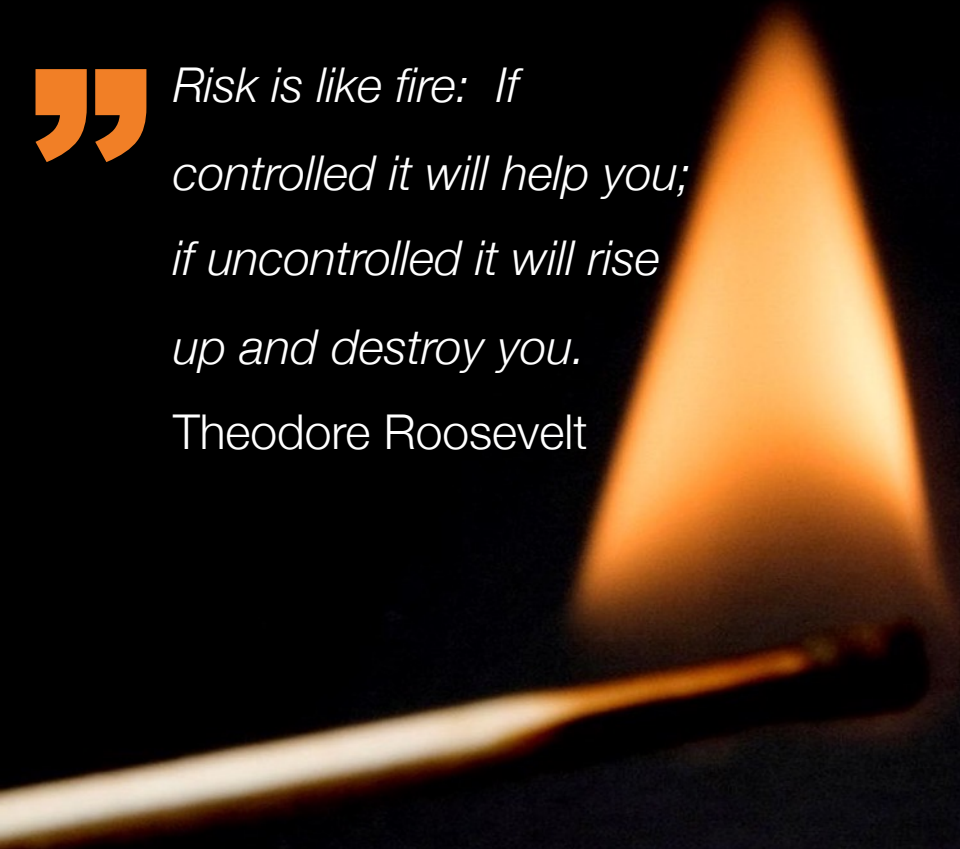


Success Requires Risk Taking, But Risk Must Be Managed



*Risk is like fire: If
controlled it will help you;
if uncontrolled it will rise
up and destroy you.*

Theodore Roosevelt



Operational Resilience Definitions

Operational resilience is a growing regulatory concern in the financial services industry. This is how the financial regulators define operational resilience:

- ❑ **UK FCA:** We define operational resilience as the ability of firms and FMI and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions.
- ❑ **EU DORA:** 'digital operational resilience' means the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality.
- ❑ **US OCC:** Operational resilience is the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.
- ❑ **Basel Committee on Banking Supervision:** The Committee defines operational resilience as the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should take into account its overall risk appetite, risk capacity and risk profile.



a·gil·i·ty

/ə'jilədē/
noun: **agility**
1. ability to move quickly and easily.
2. ability to think and understand quickly.

re·sil·ience

/rə'zilyəns/
noun: **resiliency**
1. capacity to recover quickly from difficulties; toughness.
2. ability of a substance or object to spring back into shape; elasticity.

Left-Brain

Logical and structured thinking about risk management



Right-Brain

Creative and imaginative thinking about risk management

It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts.

Sir Arthur Conan Doyle
(British Physician and Writer)

You can use all the quantitative data you can get, but you still have to distrust it and use your own intelligence and judgment.

Alvin Toffler
(American Author and Futurist)

5 stages of the risk and resilience maturity model

A sustainable risk and resilience strategy means looking to the future and mitigating risk, as opposed to putting out fires. It requires that the following risk and resilience elements are in place:

- Understand your risk.
- Approach resilience in proportion to risk.
- Tone at the top.
- Know your business and who you do business with.
- Keep information current.
- Risk and resilience oversight.
- Established policies and procedures.
- Assessment and continuous risk monitoring.
- Manage business change.

1 – Ad Hoc Risk & Resilience Maturity

1 Ad Hoc

Organizations at the Ad Hoc stage of maturity have reactive approaches to risk and resilience management at the department level. Businesses at this stage do not understand risk and exposure; few if any resources are allocated to risk and resilience. There is no ownership, monitoring, or integration of risk and resilience strategy and processes.

Characteristics of the *Ad Hoc* stage are:

- ❑ Siloed and Ad Hoc practices
- ❑ No structured and ongoing risk or resilience program
- ❑ Lack of skills and resourcing,
- ❑ No defined roles and responsibilities
- ❑ No governance structure of a risk management matrix in place
- ❑ No defined management program or risk framework
- ❑ No documented policies or procedures.
- ❑ Ad Hoc and reactive risk and continuity assessments
- ❑ Document-centric approaches
- ❑ Ad Hoc reactive approach that addresses issues as they arise
- ❑ Little to no technology in place
- ❑ No visibility, trending or analytics
- ❑ No board or senior management sponsorship

2 – Fragmented Risk & Resilience Maturity

2 Fragmented

The Fragmented stage sees departments with some focus on risk and continuity within respective areas, but they are disconnected and not working together.

Information and processes are redundant and lack integration. With siloed approaches to risk management and resilience, the organization is still very document-centric.

Processes are manual and they lack standardization, making it hard to measure effectiveness.

Characteristics of the *Fragmented* stage are:

- ❑ Tactical siloed approach to risk and continuity/resilience in different departments
- ❑ Starting to determine a roadmap, with pockets of good practice emerging
- ❑ Basic continuity plans and understanding of risk in place, and some standardization and qualification of risk
- ❑ Risk and resilience framework agreed but not implemented
- ❑ Risk and resilience governance and processes not fully embedded
- ❑ Processes are defined at the department level
- ❑ Some areas of risk management are in place but are not approached in an integrated or structured way
- ❑ No integration or sharing of continuity plans and risk between functions
- ❑ Reliance on fragmented technology and lots of documents
- ❑ Measurement and trending are difficult

3 – Defined Risk & Resilience Maturity

3 Defined

The Defined stage suggests that the organization has some areas of risk and resilience that are managed well at a department level, but it lacks integration to address risk and resilience across departments. Risk and resilience processes have the beginning of an integrated architecture and ongoing reporting. Accountability and oversight for certain domains such as business continuity, disaster recovery, and/or enterprise and operational risk management are beginning to emerge.

Characteristics of the *Defined* stage are:

- ❑ Risk and resilience management program and processes are defined with roles and responsibilities at a department level, but not across departments
- ❑ A formalized approach is in place with the framework designed and monitoring practices in place at a department level
- ❑ Risk appetite and tolerance not yet well defined or aligned, although inherent risk assessments are maturing.
- ❑ Strategic approach to governing risk and continuity is happening at a department level, but not across departments and functions
- ❑ The organizations are addressing islands and areas of risks
- ❑ Some reporting and trending at a department level

4 – Integrated Risk & Resilience Maturity

4 Integrated

In the Integrated stage, the organization has a cross department strategy for managing risk and resilience across departments and functions. Risk and resilience are aligned across several departments to provide consistent strategy, frameworks, and processes supported by a common risk and resilience information and technology architecture. However, not all processes and information are completely integrated, and risk and resilience is focused on avoiding issues and not on agility.

Characteristics of the *Integrated* stage are:

- ❑ Strategic approach to risk and resilience across departments
- ❑ Governance model agreed at board level
- ❑ Standardized risk and resiliency management strategy implemented and adopted, with documented processes
- ❑ Risks are cataloged, mapped, and monitored according to agreed and understood criteria
- ❑ Robust process monitoring measures are in place
- ❑ Appropriate skill-set and resources, with roles and responsibilities allocated
- ❑ Key departments and executives are engaged and involved.
- ❑ Silos have begun to be eliminated
- ❑ Common process, technology and information architecture across the business
- ❑ Trending and reporting across the business

5 – Agile Risk & Resilience Maturity

5 Agile

At the Agile Maturity stage, the organization has completely moved to an integrated approach to risk and resilience management across the business that includes an understanding of risk and compliance in the context of performance and objectives. Consistent core risk and resilience processes span the entire organization and its geographies. The organization benefits from consistent, relevant, and harmonized processes for risk and resilience management with minimal overhead.

Characteristics of the *Agile* stage are:

- ❑ Comprehensive governance structure with periodic meetings with board and regular governance review meetings
- ❑ Risk appetite and tolerance thresholds well defined and understood
- ❑ Risk mapping and segmentation reviewed regularly in context of change
- ❑ Cohesion across the three lines model
- ❑ Able to identify areas of improvement and measure ROI for continual improvement
- ❑ Industry best practices understood and embraced
- ❑ Enterprise view of risk and resilience across the ecosystem of the business and the extended enterprise of third-party relationships
- ❑ Risk and resilience management is integrated into roles and responsibilities
- ❑ Risk and resilience have an integrated view of performance, objectives, strategy in context of processes and services
- ❑ Risk and resilience agility is seen as a differentiator and impacts brand
- ❑ Extensive measurement and monitoring of risk in the context of business strategy and objectives
- ❑ Board and senior management led engagement, senior management champions the program

GRC 20/20's Risk & Resilience Maturity Model

Strategic Process, Information & Technology Architecture Alignment

1 Ad Hoc

Organizations at the Ad Hoc stage of maturity have reactive approaches to risk and resilience management at the department level. Businesses at this stage do not understand risk and exposure; few if any resources are allocated to risk and resilience. There is no ownership, monitoring, or integration of risk and resilience strategy and processes.

2 Fragmented

The Fragmented stage sees departments with some focus on risk and continuity within respective areas, but they are disconnected and not working together. Information and processes are redundant and lack integration. With siloed approaches to risk management and resilience, the organization is still very document-centric. Processes are manual and they lack standardization, making it hard to measure effectiveness.

3 Defined

The Defined stage suggests that the organization has some areas of risk and resilience that are managed well at a department level, but it lacks integration to address risk and resilience across departments. Risk and resilience processes have the beginning of an integrated architecture and ongoing reporting. Accountability and oversight for certain domains such as business continuity, disaster recovery, and/or enterprise and operational risk management are beginning to emerge.

4 Integrated

In the Integrated stage, the organization has a cross department strategy for managing risk and resilience across departments and functions. Risk and resilience are aligned across several departments to provide consistent strategy, frameworks, and processes supported by a common risk and resilience information and technology architecture. However, not all processes and information are completely integrated, and risk and resilience if focused on avoiding issues and not on agility.

5 Agile

At the Agile Maturity stage, the organization has completely moved to an integrated approach to risk and resilience management across the business that includes an understanding of risk and compliance in the context of performance and objectives. Consistent core risk and resilience processes span the entire organization and its geographies. The organization benefits from consistent, relevant, and harmonized processes for risk and resilience management with minimal overhead.

Issue to Departments to Enterprise Coordination and Integration

Critical elements to measure
& improve maturity

Key Risk & Resiliency Management Messages to Communicate

What it is and Why

- [ORGANIZATION] is striving to establish a distinctive competence in class risk and resiliency management
- This will enable [ORGANIZATION] to treat risks more proactively and move with agility in the financial services industry
- To do this, the R&R group will develop a culture of risk intelligence with a focus on risk and resiliency metrics
- As a result, the risk and resilience management program will enable risk intelligence through people, process and technology
- The risk and resiliency program is focused on delivering value by aggregating risk and correlating core risk elements
- We are concentrating our risk management competency expertise on 5 Risk Focus Areas
- Aligning by Risk Focus Areas allows us to work more strategically across our stakeholders groups

What This Means to Our Stakeholder Community

- Our key Risk Focus Areas allow us to evolve from risk identification, through risk analytics to risk intelligence:
 - #1 We will leverage Working Group risk through an Active Risk & Resilience Governance model
 - #2 We will focus on Enterprise Risk Analytics to develop a common risk ontology
 - #3 We will focus on Risk and Control Management to ensure best-practice mitigation is implemented for resilience
 - #4 We will focus on integrated Reporting and Information through active dashboards for stakeholders
 - #5 We will build a strong technology foundation to integrate risk, resilience and controls

What this Means to You

- This is a collaborative process between Stakeholders and the risk management team, focused on value-based initiatives
- Together we analyze each process to determine where it can be best aligned and integrated with risk themes
- Together we will create more relevant risk management value equations. product alignment and integrations

What to Expect Going Forward

- Working group participation to define risk ontology and end-end process to integrate findings, risk & remediation
- 20xx Transition to a risk management People, Process and Technology Program with more evolution to Risk Analytics in 20xx
- Opportunities to integrate new processes into the risk Technology Platform through structured Process Analysis
- Participation in a value-based, quantitative prioritization model
- On demand training as improvements to processes and systems go live
- Monthly Portfolio Report, Success Stories and updates on the risk management program and Working Group initiatives

Risk & Resilience Governance & Oversight

- Governance model is agreed at the board level and effectively communicated and supported across the organization
- Policies and procedure for risk and resilience management are fully documented and consistently applied across the organization
- Risk and resilience management framework is well defined
- Measurement and trending is now available at an enterprise view
- Risk appetite and tolerance is well defined and understood in context of objectives, processes, and services of the organization

People & Engagement

- Clear roles and responsibilities across the organization
- Skills and resources are being applied to programs
- A dedicated team is in place and recognized as a center of excellence
- Skilled subject matter experts engaged in reviews
- Training and development are embedded
- Resource is focused on strategic value-added components of the program than tactical components

Key Components in Risk & Resiliency Management

Process & Execution

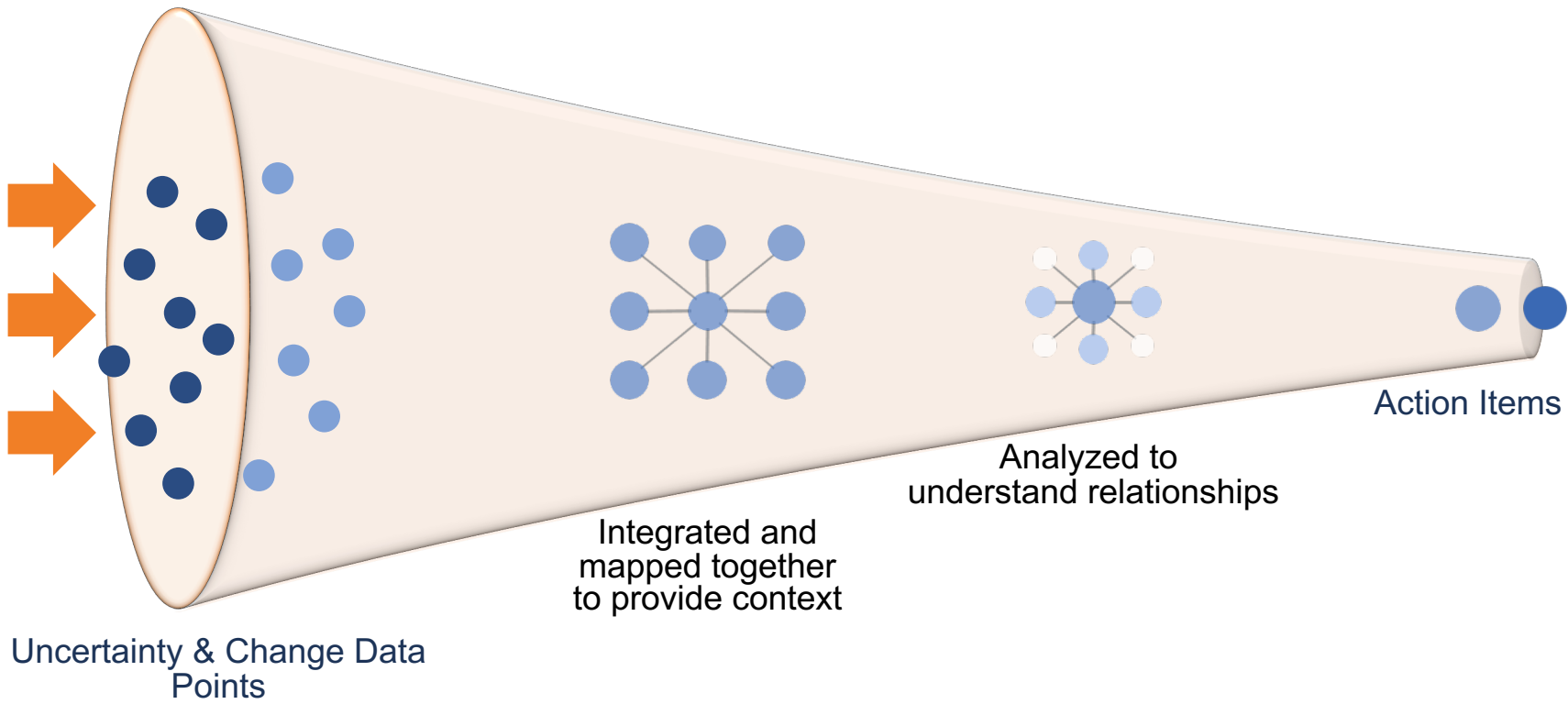
- Well defined and executed processes across the organization
- There is a single version of the truth for all risk and resilience information that is well-integrated with other business systems
- Risk assessment and monitoring processes are standardized and automated
- Segmentation and risk tiering is in place
- Clear view of inherent and residual risk at both the process and enterprise levels
- Applying a risk-based approach that incorporates critical risks and the long-tail impact
- Multiple risk categories being assessed for each department, process, and services
- Issue management is in place, and full tracking and remediation is taking place in a single system
- Ongoing monitoring is established, with changes in risk profiles automatically triggering the appropriate actions
- Clear view and controls for the extended enterprise
- Managing risk through business change

Information & Technology

- Leveraging best in class risk and resilience management software
- Risk portal for assessments, document collection, issue management and collaboration to engage front-line and operational management and risk owners
- Leveraging risk intelligence content to support automated business processes, and to support enhanced decision making

Fundamental steps to establishing your strategy

360° Identifying Risk Scenarios on the Organization

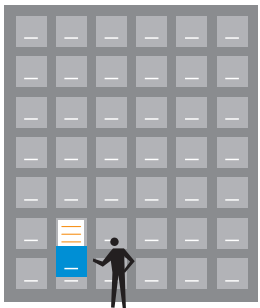


Risk & Resilience Technology Provides Risk Automation and Tracking

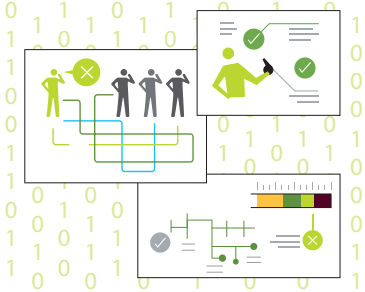
MANAGEMENT REPORTING



AUDIT TRAIL



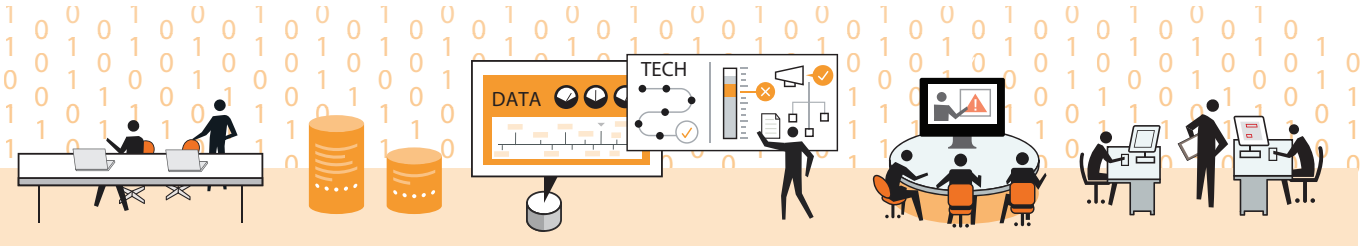
WORKFLOW & TASKS



COLLABORATION



ENFORCEMENT



Integration

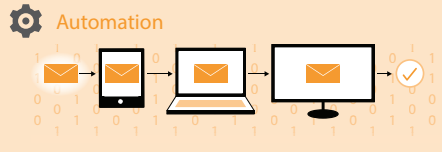
Visibility

Global Reach

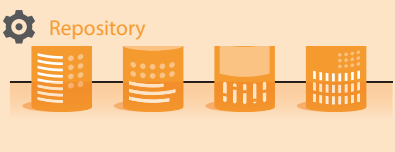
Availability



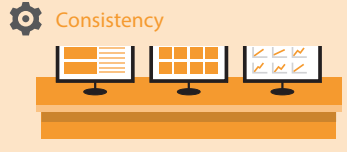
Accountability



Automation



Repository



Consistency

Components of Agile Risk & Resilience Platforms



Usability



Cost of Ownership



Configurability



Scalability



Adaptability



Integration



Analytics



A.I.
Robotic Process
Automation



Future Proof

Benefits of Automation of Risk Agility & Resiliency



Efficiency

- ✓ Time saved from manual processes
- ✓ Simplified and streamlined processes
- ✓ Reduction in reporting time
- ✓ Reduced staff to manage risk and resiliency



Effectiveness

- ✓ Less things slipping through cracks
- ✓ Audit trail of everything that happens for a complete and defensible system of record
- ✓ Allows for easier risk conversations with executives, stakeholders, and employees



Agility

- ✓ Ease of configuration to adapt to a changing risk and business environment
- ✓ Risk managed as business, processes, and roles change and evolve
- ✓ Streamlined agility in business change
- ✓ Quickly identify needs with new obligations, roles, responsibilities, tasks

Five Key Capabilities of A Next Generation Risk & Resilience Platforms

1

Risk Engagement to the Frontlines of the Organization

2

Risk Collaboration Across Roles & Departments

3

Risk Operationalization Through Defined Mapping of Business Processes

4

Risk Intelligence of External Content & Intelligence and Internal Systems & Processes

5

Risk Mobilization in Apps and Engagement for Risk Owners

The Maturity Journey

Careful planning is the key to a risk & resilience management strategy

It is critical to plan your journey by laying out the route ahead of time

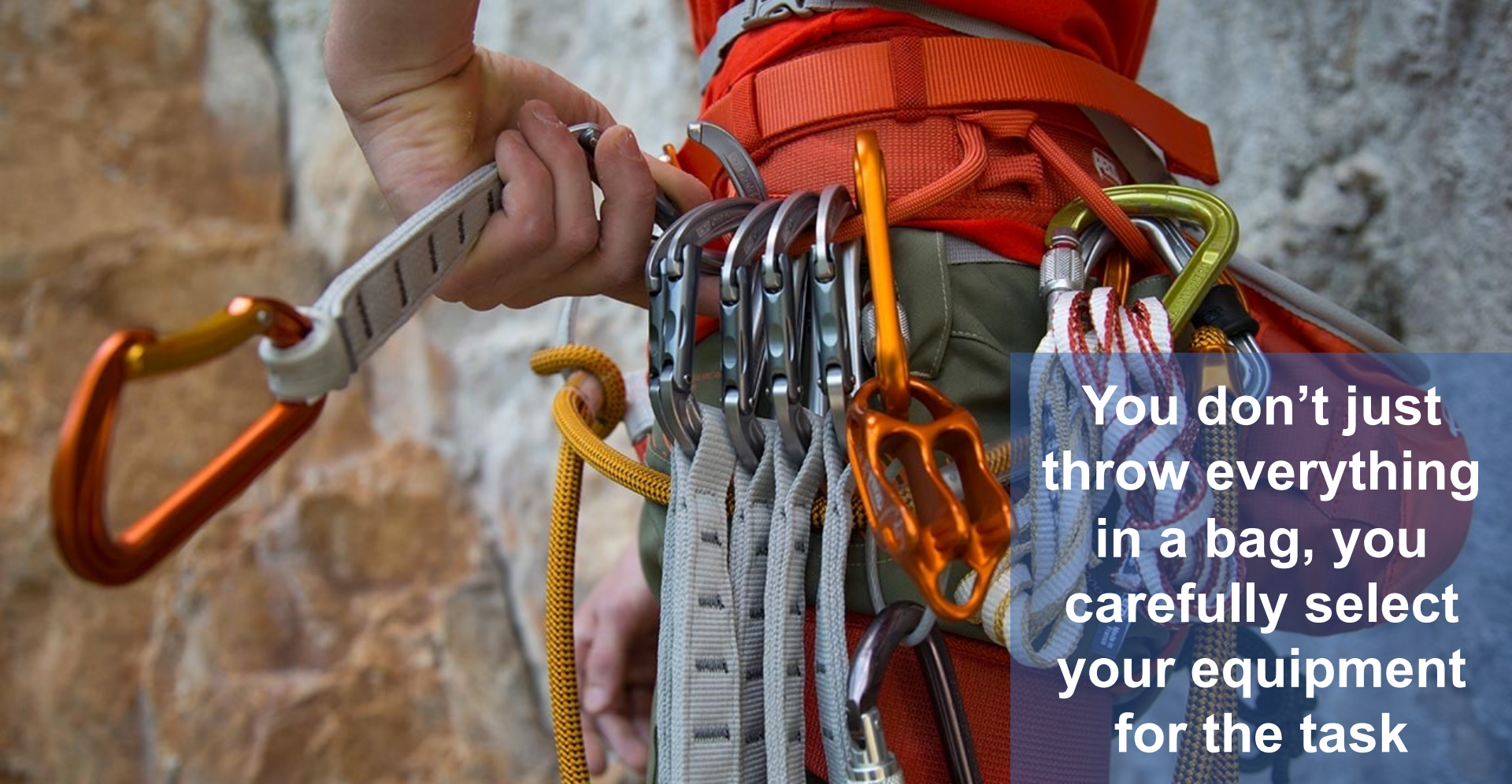


Conditioning is critical, make sure your team is ready



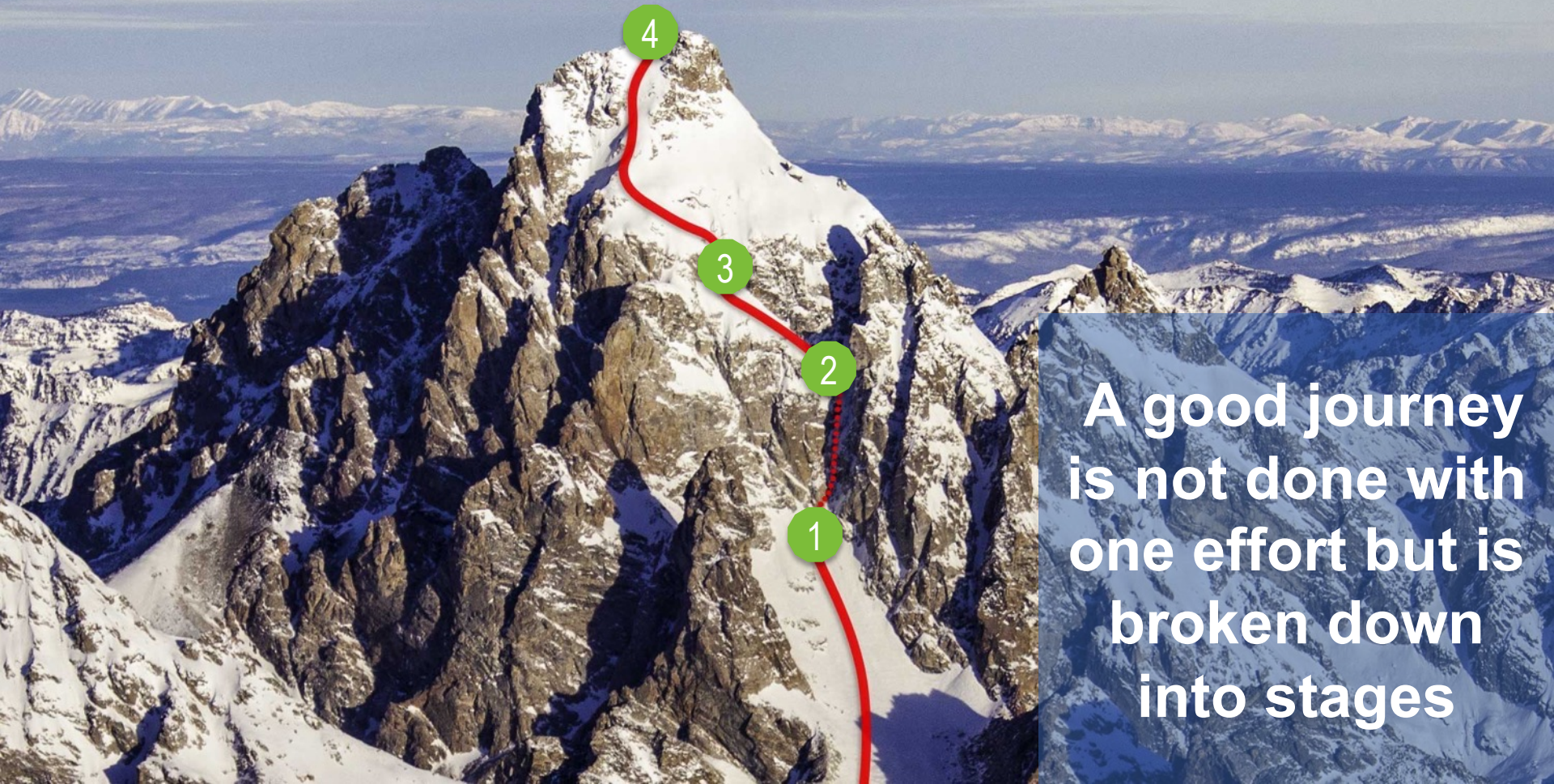
Is your organization prepared for the journey?

Select the right equipment for the risk & resilience management journey



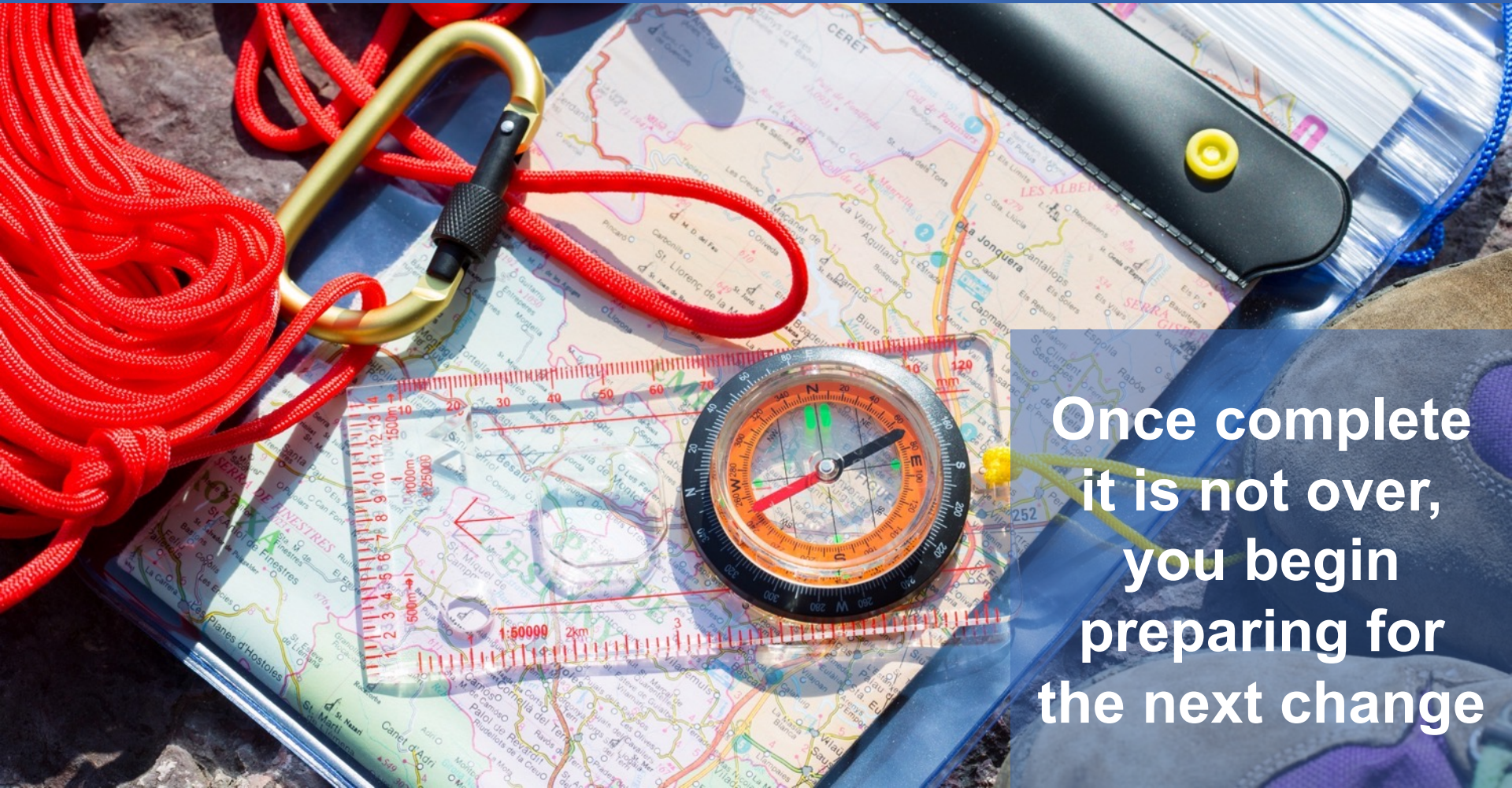
You don't just throw everything in a bag, you carefully select your equipment for the task

Tackle your risk & resilience management strategy in stages



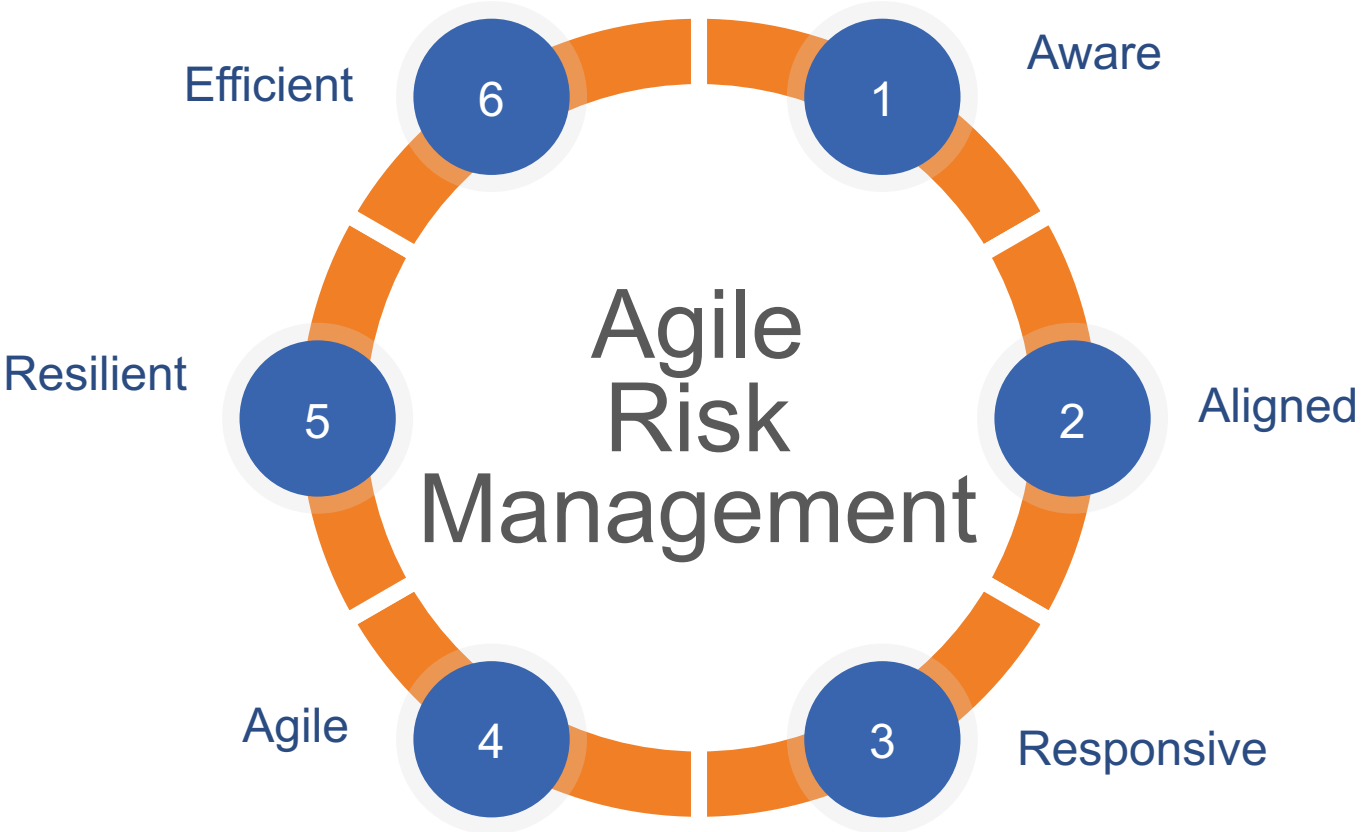
A good journey
is not done with
one effort but is
broken down
into stages

Preparing for the next journey



Once complete
it is not over,
you begin
preparing for
the next change

Benefits of 360° Contextual Awareness of Risk






Questions?

Michael Rasmussen, J.D.
The GRC Pundit & OCEG Fellow
mkras@grc2020.com
+1.888.365.4560

 [Subscribe](#) GRC 20/20 Newsletter

 [LinkedIn: GRC 20/20](#)

 [LinkedIn: Michael Rasmussen](#)

 [Twitter: GRCPundit](#)

 [Blog: GRC Pundit](#)

PRESENTATION

Governance, Risk Management & Compliance Insight