NAVEX™

How to Get Started with Information Technology & Third-Party Risk Management

- Sal Petriello, Director, IRM Product Strategy, NAVEX
- Peter Laz, MBCP, Principal, IRM Solutions, NAVEX

Agenda

- Welcome and Introductions
- Risk Management Level-Set
- 7 Step Checklist for ITRM and TPRM
- Wrap Up
- Q&A

Presenters

Sal Petriello

Director
IRM Product Strategy

- 30+ Years as a Practitioner and Advisor
- Operations and Service Leader in Financial Services and Healthcare Industry
- Joined NAVEX, November 2021
- Integrated Risk Management Product Strategy and Marketing

Peter Laz

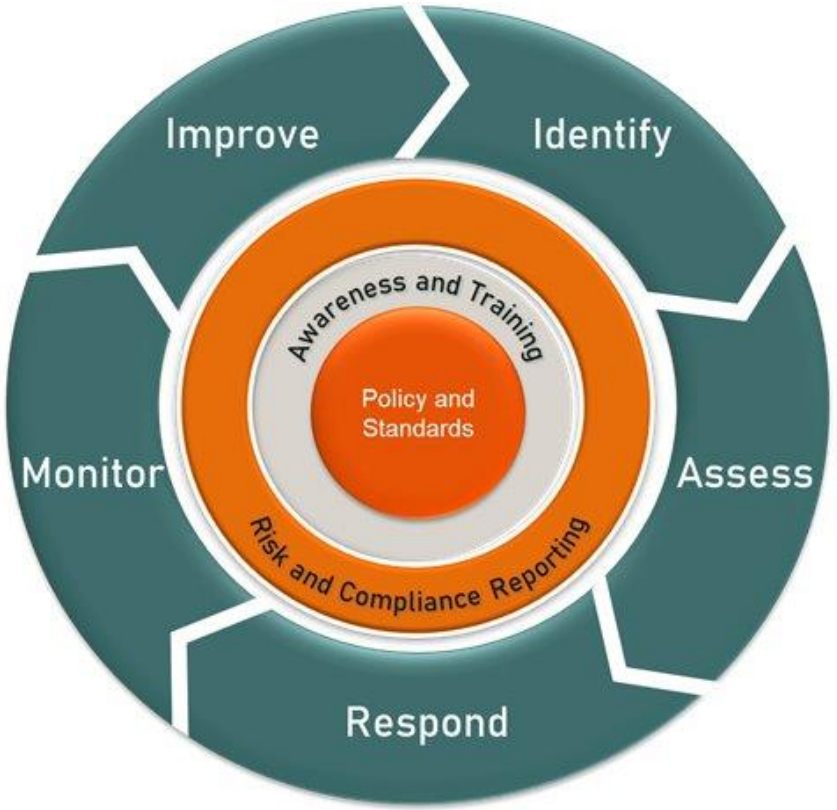
Principal
IRM Solutions

- 35 years in Operational Risk
- Practitioner and Advisor
- DRJ Executive Council
- Joined NAVEX, Jan 2020
- Lead Integrated Risk Management roadmap by partnering with Customer Success, Sales, Marketing and Product

Risk Management Context

Risk:
The possibility of danger, harm or loss

- When businesses do not effectively manage risk, the adverse events cause:
  - Degraded brand reputation
  - Decreased profits
  - Business failure

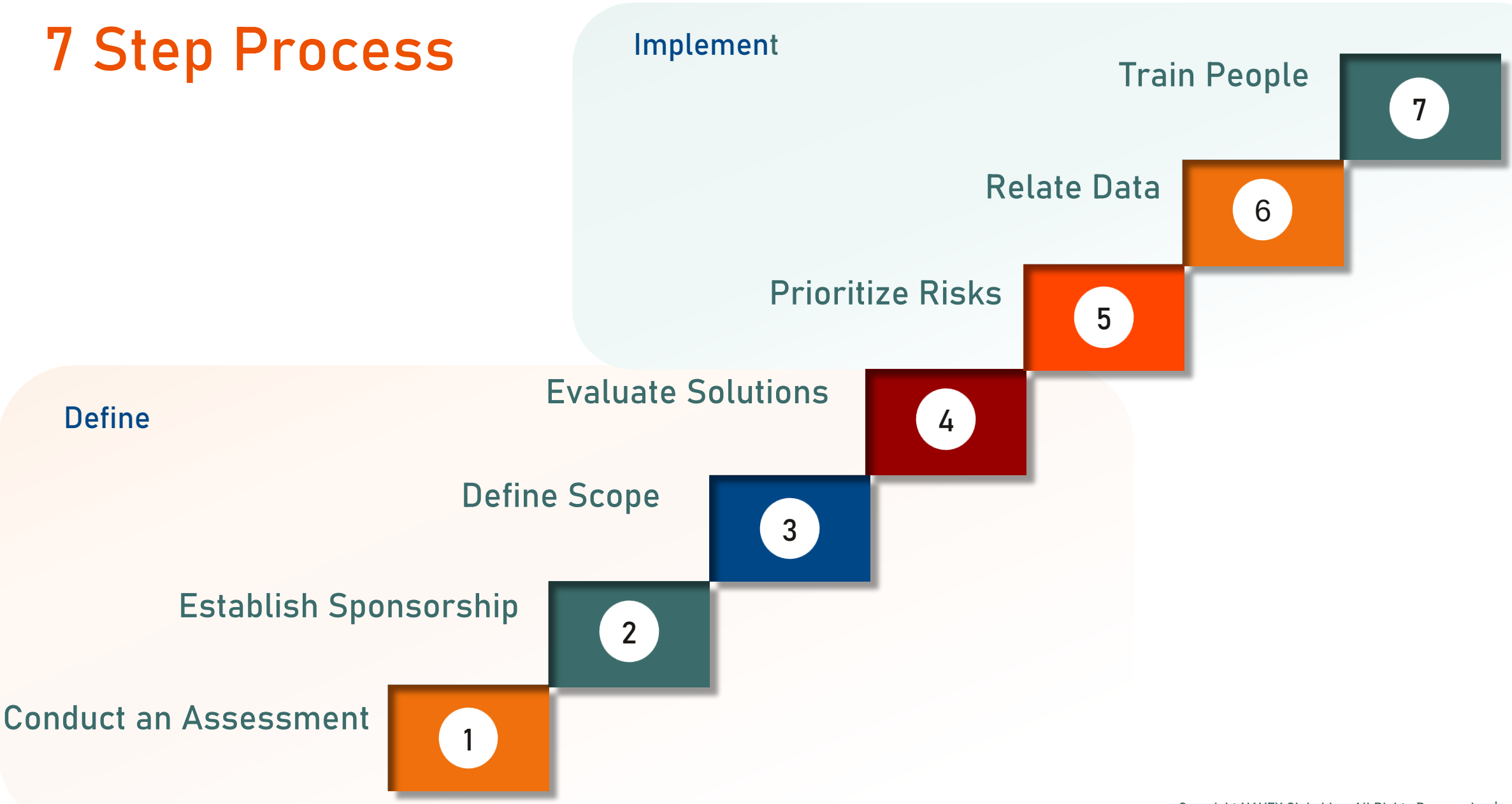


NAVEX™

Baseline Definitions

Term	Definition
Inherent Risk	The amount of risk that exists in the absence of controls.
Residual Risk	The amount of risk that remains after controls are applied.
Risk Response (Treatment, Disposition)	The selected decision of action to address the residual risk. Accept, Assign, Mitigate or Avoid
Risk Register	A repository of risks that pose a threat to an organization.
Control Register	A repository of the actions that will reduce the inherent risk of a threat.
Risk Category	The classification of risks which provide an overview of the underlying and potential risks.
Risk Appetite	The amount of risk an organization is willing to accept to achieve its goals.
Risk Tolerance	The acceptable deviation from the organization's risk appetite.

7 Step Process



Define Phase

Step	Comments	Outcome
1 - Assessment	• Begin with the end in mind – program goals • General capabilities assessment • Be clear on your organization's needs	• High-level Roadmap • Gaps • A clear understanding and point of focus for your *future* IT and TPRM programs
2 - Sponsorship	• Tone at the top is critical success factor • Establish executive jurisdiction • Frame elements for "culture of compliance"	• Executive-level Ownership • Roadmap Support • Program "Air-Cover"
3 – Scope	• Project goals/deliverables/features/functions/tasks • Resources required to actualize plans • Deadlines/costs	• Program owner • Parameters, timeline • Policy • Roles & responsibilities
4 - Solutioning	• Ensure potential solutions align with program objectives • Adoption – ease of use • Scalability	• Selection of application/system to manage the program

NAVEX™

Implement Phase

Step	Comments	Outcome
5 – Prioritize Risks	• Organizational hierarchy, risk/control registers, top risks per category • Identify key risks to evaluate at beginning of the program • 80/20 Rule	• Foundational structures & data • Baseline risks & controls
6 – Relate Data	• Establish relationships between elements to perform the risk assessments (e.g., processes, applications, sites, etc.) • Enable “one to many” relationships • Earmark importance of relationships	• Risk system is prepared to perform the risk assessments at an appropriate level • Relationships allow for aggregation of data at the enterprise Level
7 –Train People	• Position stakeholders to actively support risk assessment process • Provide “bigger picture” context and reason for individual tasks for involved teams • Integrate with your organizations other training platforms (e.g., LMS)	• People resources are prepared to start conducting the risk assessments

NAVEX™

Call to Action

- Identify a champion
- Lay some groundwork
  - ❑ Connect risk program goals to corporate objectives
  - ❑ Identify and engage stakeholders
  - ❑ Establish time commitments
  - ❑ Document expected outcomes and value
- Customize activities to align with your culture

NAVEX™

Wrap Up

- Importance of a structured program
  - Businesses that do not effectively manage risk are subject to degraded reputation, profits and business failure
- An executive champion is a critical success factor
- This is not a “light-switch”
- These 7 Steps are a guide - there is no one-size-fits all approach to risk management, and this must be customized for your business

NAVEX™

Thank you.

NAVEX™

