



DIGITAL TRUST WORLD

An ISACA® Conference

ERM Governance in a Digital World – A Transformative Case Study

Joseph W. Mayo, PMP, PMI-RMP, CRISC, RIMS-CRMP, CMMI Associate

DISCLAIMER



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of ISACA or any other co-sponsors. ISACA does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2023 ISACA or its affiliates. The ISACA logo and other trademarks are proprietary. All rights reserved.

Learning Objective #1

- Identify and describe best practices for implementing an ERM program that aligns with industry standards and best practices.



**DIGITAL
TRUST
WORLD**

An ISACA® Conference



Learning Objective #2

- Describe critical success factors for ERM Governance in today's highly disruptive digital world.



**DIGITAL
TRUST
WORLD**

An ISACA® Conference



Learning Objective #3

- Define a future-proof ERM Governance Model that easily adapts to the changing digital world.



**DIGITAL
TRUST
WORLD**

An ISACA® Conference



Learning Objective #4

- Recognize the line of demarcation between managed risk and emerging risk for their organization and learn how to establish key risk indicators (KRI) to provide early warning about the birth of an emerging risk.



**DIGITAL
TRUST
WORLD**

An ISACA® Conference



About Me



BS/IT, MIS

PMP, PMI-RMP, RIMS-CRMP, CRISC, CMMI Associate

Author

- Cultural Calamity – Culture Driven Risk Management Disasters and How to Avoid Them
- Chaos to Clarity – The Tao of Risk Management

Creator of the Risk Hurricane - organizational culture barometer to indicate culture traits that can lead to disastrous results

joseph.mayo@jwmc-llc.com

@TaoOfRisk

<https://www.linkedin.com/in/josephmayo/>



Case Study Introduction



**DIGITAL
TRUST
WORLD**

An ISACA® Conference

Organization with a \$293M annual operating budget

ERM implementation was the Senior Executive's top priority

Allocated ~\$2M dollars to ERM implementation in year 1

Dedicated ERM team of 3 customer personnel, 3 fulltime contractors and 3-5 part-time contractors

Polling Question



How many risk contexts / categories does your organization have?

- Less than 10
- 10 – 20
- 21 – 50
- More than 50

ERM Implementation Best Practices

Tone at the top is the most important critical success factor

No single standard, framework or document will deliver ERM

- Process guidance
- Governance Framework
- Technical Standards
- OMB Circular A-123 and OMB A-123 Playbook is a good start
 - Borrows heavily from ISO 31000, UK Orange Book, COSO and others
 - https://www.osec.doc.gov/opog/privacy/Memorandums/OMB_Circular_A-123.pdf
 - <https://www.doi.gov/sites/doi.gov/files/erm-playbook-2022-update-final-508-compliant.pdf>

Risk Categories Across the Enterprise

1. Acquisition
2. Budget Authority
3. Budget Execution
4. Business
5. Contracting
6. Cost
7. Customer
8. Cyber Security
9. Data
10. Efficient Operations
11. Financial Risk
12. Funding
13. General
14. Human Capital Risk
15. Innovative Sustainable E-commerce
16. Institutional
17. Integration
18. O&M
19. Operational
20. Operational Expertise
21. Operations
22. Organizational and Change Management
23. Performance
24. Performance-based Logistics
25. Privacy
26. Programmatic
27. Programmatic Risk
28. Project Management
29. Project Team
30. Reporting
31. Reputation Risk
32. Requirements
33. Security
34. Staffing (FTE Days)
35. Stakeholder I/F
36. Strategic
37. Support
38. Technical Interface (I/F)
39. Technical Performance
40. Technology
41. Technology Risk
42. Training
43. Workforce Skills & Capabilities

Polling Question



Does your organization currently have a risk operations center (ROC)?

- Yes
- No
- I don't know what a ROC is

Risk Categories Across the Enterprise

Board defined 3 risk categories

Independent Audit defined 4 categories

- Only 1 aligned with Board categories

Headquarters defined 9 categories

- Only 1 aligned with Board categories

Divisions defined 9 categories

- 1 category aligned with Board categories
- 4 categories aligned with HQ

Internal Audit defined 13 categories

- 1 category aligned with Board categories
- 1 category aligned with HQ

Risk Categories Across the Enterprise



DIGITAL TRUST WORLD

An ISACA® Conference

| Board | Independent Audit | Headquarters | Division | Internal Audit | Program 1 | |
|-------------|-------------------|------------------------|------------------------|----------------|---------------------|-------------------|
| Strategic | Strategic | Strategic | Strategic | Strategic | Acquisition | |
| Operational | Operations | Technology Risk | Efficient Operations | Technology | | |
| | | | | Integration | Technical Interface | |
| | | | | Security | Security | |
| | | | | Privacy | CyberSecurity | |
| | | Programmatic Risk | | | Privacy | Privacy |
| | | | | | | Customers |
| | | | | | | Performance-based |
| | | | | | | Logistics |
| | | | | Support | | |
| | | | | O&M | | |
| Operational | | Safety / Security Risk | Safety / Security Risk | | Safety | |

| Board | Independent Audit | Headquarters | Division | Internal Audit | Program 1 | |
|---------------|-------------------|--------------------|-----------------------------------|--------------------------------------|---------------------|-----------------|
| Operational | Operations | Technology Risk | Efficient Operations | Technology | | |
| | | | Integration | Technical Interface | | |
| | | | Security | Security | | |
| | | | Privacy | CyberSecurity | | |
| | | Programmatic Risk | | Customers | | |
| | | | | Performance-based | | |
| | | | | Logistics | | |
| | | | | Support | | |
| | | | | O&M | | |
| | | | | | | |
| Institutional | Operations | Programmatic Risk | Innovative Sustainable E-commerce | Project Team | Performance | |
| | | | Requirements | Technical Performance | | |
| | | | Project Management | Programmatic | | |
| | | | Data | | | |
| | | | Business | General | | |
| | | Human Capital Risk | Workforce Skills & Capabilities | Organizational and Change Management | Staffing (FTE Days) | |
| | | | Operational Expertise | | Training | |
| | | | | | Contracting | |
| | | Financial Risk | | Cost | Cost | |
| | | | | | Funding | |
| | | | | | Budget Authority | |
| | | | | | Budget Execution | |
| | | Reporting | Reputation Risk | Reputation Risk | | Stakeholder I/F |
| | | Compliance | Legal Risk | Legal Risk | | Documentation |
| | | | Policy / Governance Risk | Policy / Governance Risk | | Governance |
| | Programmatic Risk | | Project schedule / resources | Schedule (Days) | | |



DIGITAL TRUST WORLD

an ISACA® Conference

Risk Categories Across the Enterprise

| | Board | Independent Audit | Headquarters | Division | Internal Audit | Program 1 | | |
|-----------------|----------------|-------------------|--------------------------|------------------------------|-----------------------------------|--------------------------------------|---------------------|---------|
| Mission Risk | Strategic | Strategic | Strategic | Strategic | Strategic | Acquisition | | |
| | Operational | Operations | Technology Risk | Efficient Operations | Technology | | | |
| | | | | | Integration | Technical Interface | | |
| | | | | | Security | Security | | |
| | | | | | | CyberSecurity | | |
| | | | | | Privacy | Privacy | | |
| | | | | | | Customers | | |
| | | | Programmatic Risk | | | Performance-based | | |
| | | | | | | Logistics | | |
| | | | | | | Support | | |
| | | | | | | O&M | | |
| | Financial Risk | Institutional | Operations | Programmatic Risk | Innovative Sustainable E-commerce | Project Team | Performance | |
| | | | | | Requirements | Technical Performance | | |
| | | | | | Project Management | Programmatic | | |
| | | | | | Data | | | |
| | | | | | Business | General | | |
| | | | | | | | | |
| | | | | Human Capital Risk | Workforce Skills & Capabilities | Organizational and Change Management | Staffing (FTE Days) | |
| | | | | | Operational Expertise | | Training | |
| | | | | | | | Contracting | |
| | | | | | Financial Risk | | Cost | Cost |
| | | | | | | | | Funding |
| Reputation Risk | | | | | Reporting | Reputation Risk | Reputation Risk | |
| | | Compliance | Legal Risk | Legal Risk | | Documentation | | |
| | | | Policy / Governance Risk | Policy / Governance Risk | | Governance | | |
| Schedule Risk | | | Programmatic Risk | Project schedule / resources | Schedule (Days) | | | |
| Quality Risk | | | | | | | | |
| Safety Risk | Operational | | Safety / Security Risk | Safety / Security Risk | | Safety | | |



DIGITAL TRUST WORLD

An ISACA® Conference

Polling Question



Has your organization implemented continuous governance?

- Yes
- No
- I don't know

ERM Governance Model

| | | |
|--------------------|----------------------------------|-----------------------------------|
| ERM Infrastructure | Policies, Processes & Procedures | IT, Services & Applications |
| ERM Mechanics | Executive Steering Committee | ERM Advisory Committee(s) |
| | ERM Adjudication Board | Risk Review Board |
| | Risk & Strategy Committee | Situational Awareness |
| Quality Audits | | |
| ERM Oversight | Process Audits | Culture Audits |
| | Goal Alignment | Capacity & Capability Assessments |
| | Personnel and Culture | Define & Maintain Risk Culture |

Environment Scanning
 Risk Operations Center (ROC)
 Pre-mortems
 Future Casting

Future Proofing



DIGITAL TRUST WORLD

An ISACA® Conference

Where Does Emerging Risk Begin?



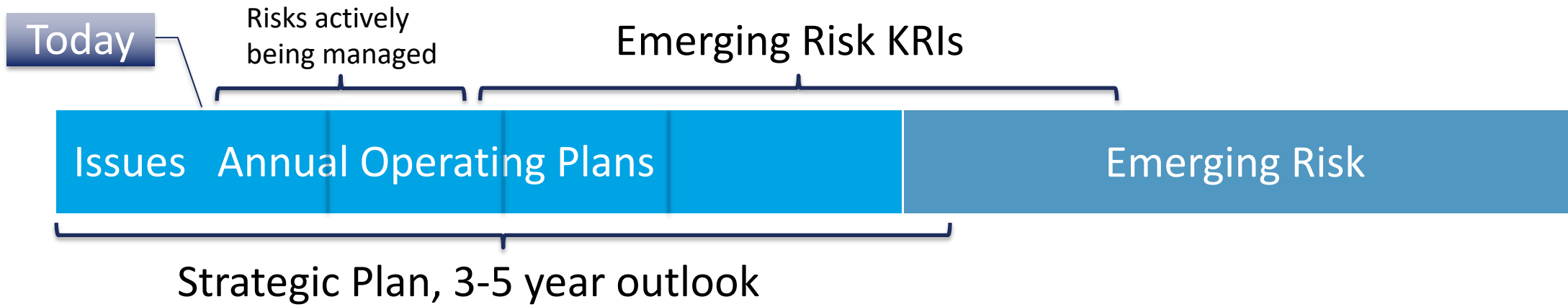
DIGITAL TRUST WORLD

An ISACA® Conference

Emerging risks are outside of the current annual operating plan

Emerging risk management requires effective KRIs

High performance organizations will be managing emerging risks 5-10+ years out



Polling Question – Closing Topic

Choose one of the following for the closing topic?

- Customer concerns about implementation
- Implementation schedule
- Pre-mortem details



**DIGITAL
TRUST
WORLD**

An ISACA® Conference

Closing Topic



[Customer concerns about implementation](#)

[Implementation schedule](#)

[Pre-mortem details](#)



Customer concerns about implementation

Governance model is intimidating

Organizational Change Management

Limited resources for such a large undertaking



**DIGITAL
TRUST
WORLD**

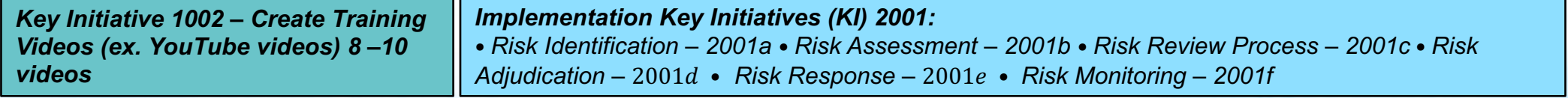
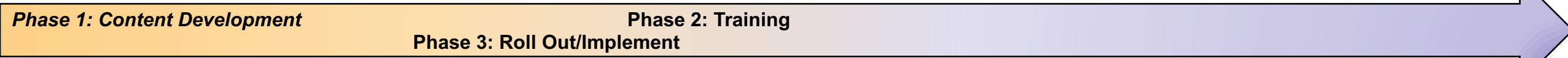
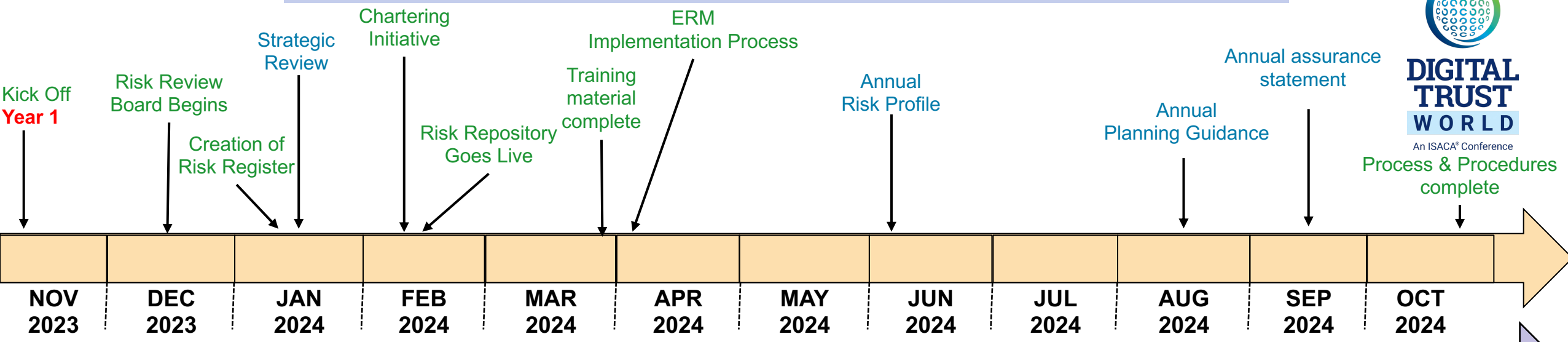
An ISACA® Conference

Implementation Schedule – Year 1



DIGITAL TRUST WORLD
An ISACA® Conference

Process & Procedures complete



Risk Management Activities: Identify, Assess, Review, Adjudicate, Respond, Monitor (on-going)

Develop and Retain Risk Management Talent (on-going) | **Define and Maintain Risk Culture (on-going)**

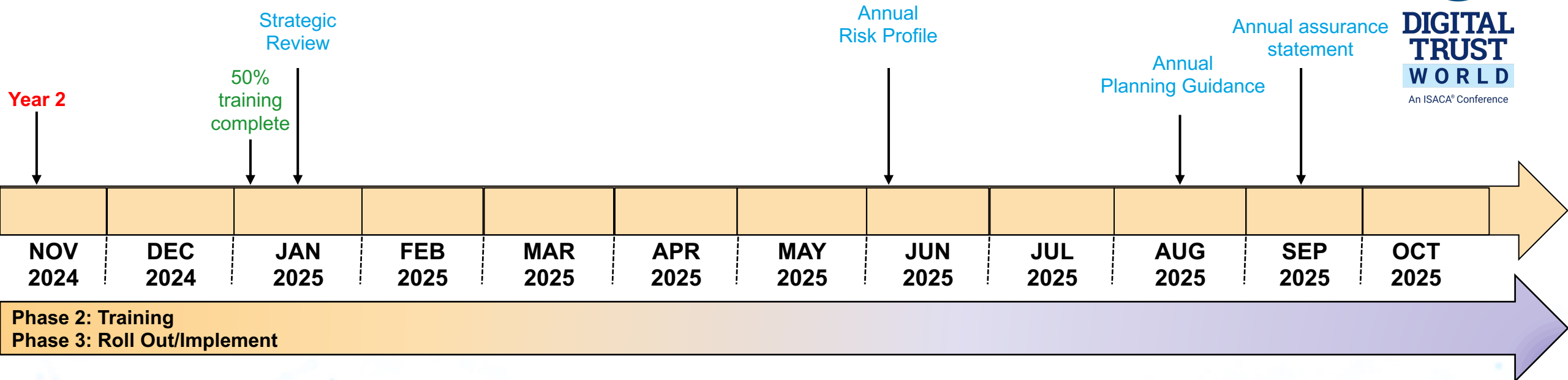
Policies, Processes & Procedures | **IT, Services & Applications**



Implementation Schedule – Year 2



DIGITAL TRUST WORLD
An ISACA® Conference



Emerging Risk, Risk Scanning

Emerging Risk, Risk Scanning

Risk Process Audits

Risk Quality Audits

Risk Culture Audits

Risk Management Activities; Identify, Assess, Review, Adjudicate, Response, Monitor (on-going)

Develop and Retain Risk Management Talent (on-going) Define and Maintain Risk Culture (on-going)

Pre-mortem details



**DIGITAL
TRUST
WORLD**

An ISACA® Conference

- Imagine hypothetical future scenarios where a strategic goal or objective has failed
- Facilitated risk management technique used to anticipate and respond to potential failures or problems before they occur, in other words envision the future
- Uses prospective hindsight, to reduce uncertainty and facilitate team brainstorming
- Helps identify risks, potential failure scenarios, potential pitfalls in the decision-making process
- Helps identify blind spots in the strategic plan or market projections
- Enhances decision-making, improve outcomes, and increase the overall chances of success
- Consider involving a Futurist in pre-mortems to set the stage and drive futuristic thinking

Questions?



**DIGITAL
TRUST
WORLD**

An ISACA® Conference

joseph.mayo@jwmc-llc.com

@TaoOfRisk

<https://www.linkedin.com/in/josephmayo/>