Business Driven Risk Management in a Digital World

Ken McPherson, CEO

icebergnetworks.com
Today’s Agenda

- About Iceberg
- What is digital risk management?
- What’s most important to the business – Risk Posture
- What are the types of risks involved in digital transformation projects?
- Three key use cases
- Value of the business translation layer
- How to communicate digital risk to all stakeholders
- Keys to success in implementing a digital risk management program
- Questions and Answers
About Iceberg Networks

- **13+** Years in Business
- **100+** Successful Deployments
- **Financial Services, Government, Healthcare, Manufacturing and Retail**
- **20+** Years of Risk Management Experience for each of our Management Consultants
- **30+** GRC/IRM Experienced Technical and Certified Resources
- **100%** Focus on Integrated Risk
Digital Transformation

Digital transformation creates new opportunities to thrive and compete—but it also creates new risk.

Digital business typically involves fast-moving projects supported by processes that require a multitude of different applications, expanding the points of risk and the stakes for the organization.

The key to seizing the opportunities is managing these risk in critical areas.

In 2022, organizations are projected to spend nearly $2 trillion on digital transformation, according to the International Data Corporation, spurred by a proliferation of new digital technologies and a fear of disruption by tech-enabled competitors. (Deloitte 2019)
A risk management strategy provides a structured and coherent approach to identifying, assessing and managing risk. It builds in a process for regularly updating and reviewing the assessment based on new developments or actions taken.
What is Digital Risk Management?

Identifying WHAT MIGHT HAPPEN?
Changing Landscape for IRM

Culture
New Technologies
New People
New Processes

= All impact the business in NEW ways
IRM Evolution for Digital Transformation

- Cyber
- 3rd Party Risk
- Operational Resilience
- Enhanced Dashboards and Reporting
#2 3rd Party Risk in now “Nth” Party Risk

Cloud

Managed Services

Third Party suppliers and THEIR environments
Hackers used stolen credential from a HVAC contractor to breach Target's systems and steal customer credit card and personal information costing Target over $18.5M
#3 Operational Resilience

Our Industry has agreed breaches are going to happen.

To what extent is your organization capable of responding to and minimizing downtime? So that your service is not materially impacted, or your product delivery delayed.

- Requires full understanding of the operational and business processes
- Requires effective and tested business resiliency plans
- Requires effective and tested crisis management solution
#4 Enhanced Dashboards and Reporting
Critical piece to effectively communicate digital risks to the organization’s decision makers!
Business Translation Layer

- BOARD
- EXECUTIVE
- BUSINESS
- AUDIT
- REGULATORS

- COMPLIANCE RISK
- PRIVACY & GDPR
- BUSINESS CONTINUITY
- AUDIT
- POLICY MANAGEMENT
- REGULATORY CHANGE MANAGEMENT
- CYBER RISK
- OPERATIONAL RISK
- VENDOR RISK
- SECURITY ASSESSMENTS
- IT RISK
Keys to Success

- Get continuous executive support – effective steering committee
- Get Stakeholder/User/Business to weigh in – allows them to buy-in
- Break down the organization and data silos – It’s Time!
- Focus on Outcomes (vs. features)
- Cultivate a risk culture – Show the Organization is serious about digital risk management
Questions and Answers
Thank you.