MEASURING TECHNOLOGY SUCCESS
CONNECTING RISK, GOVERNANCE, AND METRICS

RSM - WINTRUST

APRIL 9, 2018

AGENDA

- Today's business leaders are required to effectively oversee IT and Cyber Security — increasing value and performance while decreasing risk. Board's role is to provide oversight over those areas and help drive better risk management. Learn how to use industry standard frameworks to better inform your leaders and the board.

- By the end of this course, you will be able to:
  - Leveraging enterprise risk management and industry leading IT / IS frameworks to evaluate and direct enterprise IT
  - Transforming IT metrics into risk dashboards to report and inform Executives and the Board
  - Case Study: How Wintrust linked their ERM program to the FFIEC CAT framework to measure success

INTRODUCTIONS

Hussain T. Hasan
Principal
RSM US LLP

Jack Burback
Deputy CISO
Wintrust Financial

Patricio Cadena
Manager
RSM US LLP

Alex Noonan
Senior Associate
RSM US LLP

AT A GLANCE

WINTRUST

Financial services holding company providing community banking, wealth management, commercial insurance premium financing, and mortgage origination

$18+ billing in assets

15 wholly owned banking subsidiaries

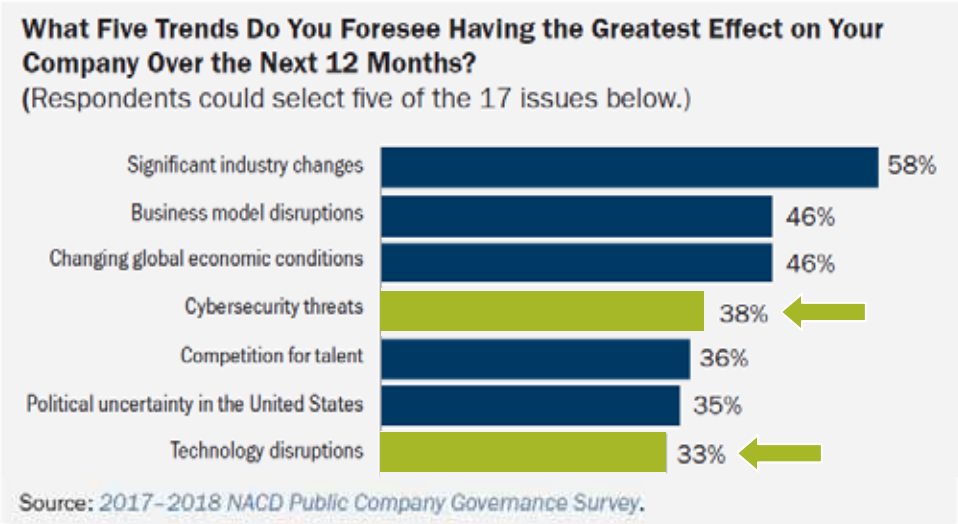
RSM

Fifth largest audit, tax and consulting firm in the US and the largest firm world-wide focused on serving the middle market

120+ countries

41,000+ people

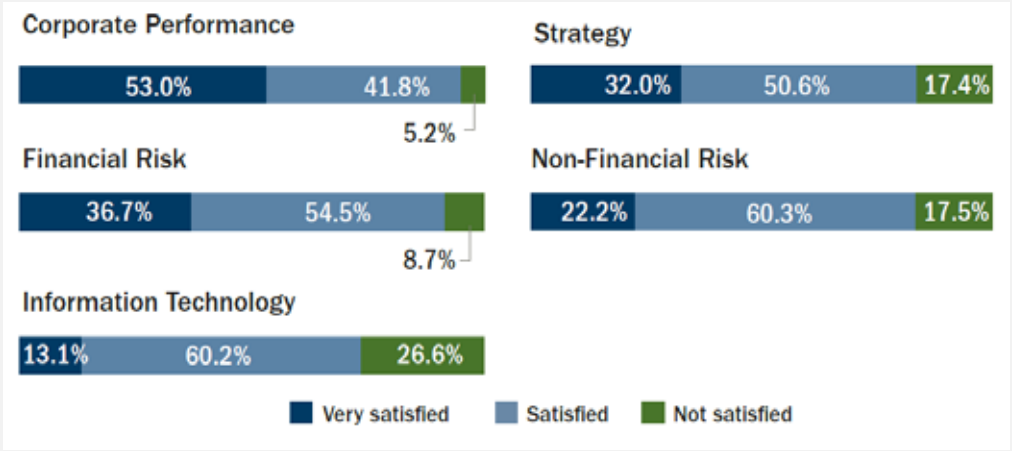
WHAT DO PUBLIC COMPANY BOARDS BELIEVE THE TOP BUSINESS TRENDS WILL BE IN 2018?



- **Cybersecurity Risk Becoming a Boardroom Staple**
- Concern has risen with widely reported breaches
- Increasing need for clearer and more complete, relevant, and timely assurance regarding the organization's ability to identify, manage, and respond to cyber risks

BOARD MEMBERS ARE NOT SATISFIED WITH THE INFORMATION PROVIDED BY IT

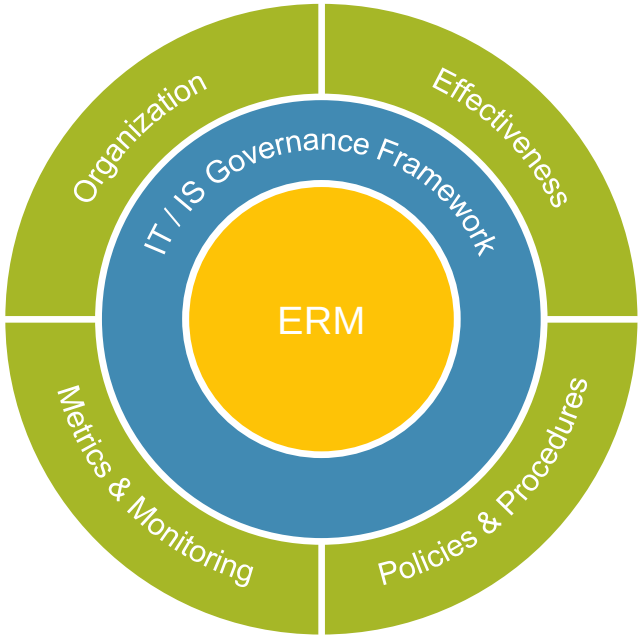
Please assess the quality of the following information provided to the board by management:



- Information is either too much or too granular and without prioritization
- More likely to become overwhelmed and miss critical risks
- Often times, Board composition does not include IT expertise
- Only **49 percent** of board respondents are confident or very confident that management can effectively manage cyber risk

Source: NACD Mitigating Board Information Risk

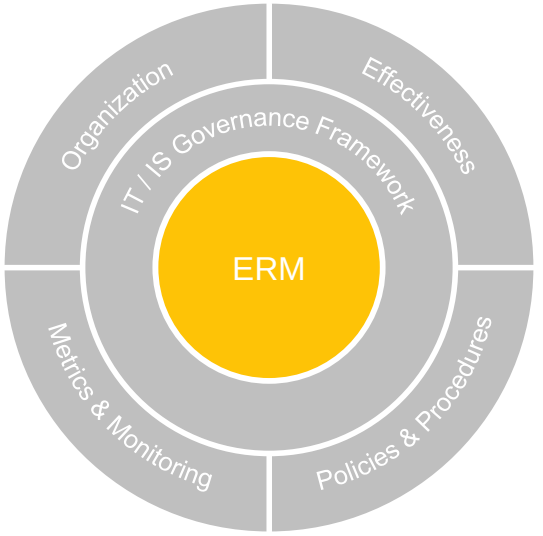
HOW DO ORGANIZATIONS IMPROVE THE INFORMATION AND DATA PROVIDED TO THE BOARD AND EXECUTIVE MANAGEMENT?



- Align IT / IS risk governance to organization's Enterprise Risk Management processes
- Enables IT / IS to measure risks as part of organizational reporting and review structure
- Enables policy/procedure development and department structure alignment with ERM

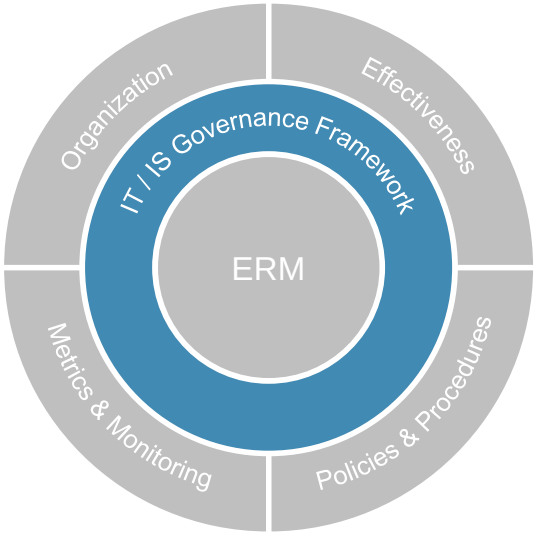
BEGIN WITH ENTERPRISE RISK MANAGEMENT MODEL

- Enterprise Risk Management (ERM) provides the Board and Executive leadership visibility into risks across the organization and their impact on objectives
  - Provides opportunity to **identify** emerging risks
  - Provides opportunity to **prioritize** response
  - Provides opportunity to **track** mitigation effectiveness
- Measures and represents the health of the company
- ERM model is specific to company profile
- Risk appetite is established and incorporated into operations



CHOOSE THE RIGHT GOVERNANCE FRAMEWORK

- IT/IS governance is a framework to ensure that IT/IS investment and output are supporting organizational objectives and goals
- Utilize the framework to establish gaps, risks and priorities
- Governance framework is specific to the needs of the organization
  - Industry
  - Regulatory
  - Size
  - Structure
  - Focus
  - Maturity

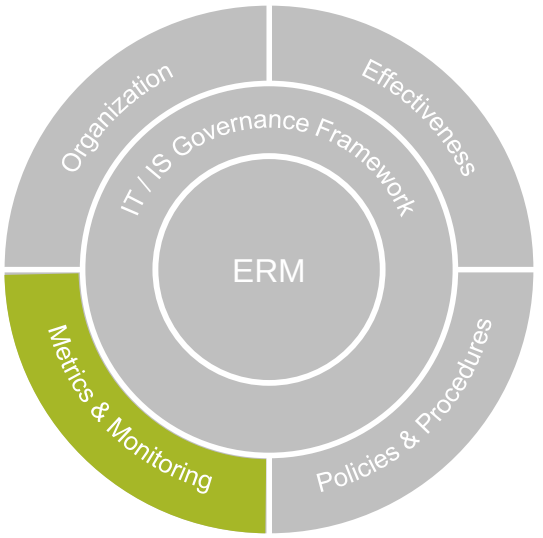


MEASURE AGAINST THE FRAMEWORK

- Performance vs Risk Indicators
  - KPIs measure the **actions** that lead to a result – **Operational**
  - KRIs measures the **results** from your actions – **Strategic**

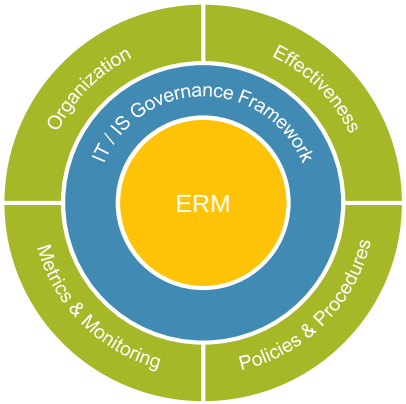
- Begin with most critical risks
  - Many governance frameworks include recommended KPIs and KRIs
  - Non-compliance to regulatory requirements and/or policy
  - Start with the data you have - generate, iterate and automate

- Metric thresholds should align with organizational risk appetite



Enterprise Risk Management

- Board and Executive visibility into organizational risks
- IT/IS adopts ERM framework processes



IT / IS Governance Framework

- Select a framework for fit and purpose
- Aligns IT risk governance to organizational priorities

Organization

- Framework informs structure and job descriptions
- Leverage framework to identify gaps

Metrics & Monitoring

- Concisely inform the Board of critical risk areas
- Start with highest risk KPIs/KRIs that can be produced today

Effectiveness

- Framework provides the basis for improving maturity
- Focus improvements on critical risk areas

Policies & Procedures

- Framework informs policy and procedure content
- Describe the "what" and "how" to deliver on the framework

CASE STUDY

HOW WINTRUST LINKED THEIR ERM PROGRAM TO THE FFIEC CAT FRAMEWORK TO MEASURE SUCCESS

WINTRUST COBIT ASSESSMENT AND ROADMAP

The COBIT governance framework was selected to be used in an initial assessment of Wintrust's IT organization

1. Weighted each COBIT process relative to size and industry
2. Assessed IT governance relative to the COBIT framework

Assessment

- All **policies & procedures**
- Existing **organization** structure
- **Monitoring** and metrics (KPI/KRI)
- Process control **effectiveness**

3. Evaluated and documented gaps for each process
4. Created roadmap to address the identified gaps

Analysis

- Detailed observations and recommendations for each COBIT process

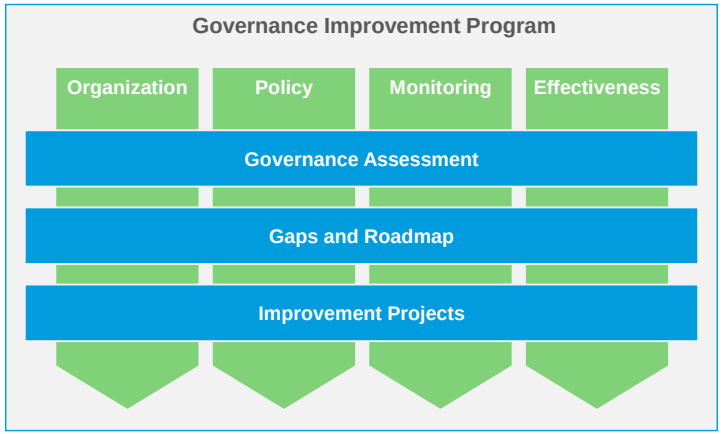
Roadmap

- Developed a prioritized and phased roadmap focused on monitoring and effectiveness

GOAL: DEVELOP AN EFFICIENT MONITORING AND RISK REPORTING PROCESS TO CONCISELY INFORM BOARD MEMBERS

1. **Incorporate InfoSec into ERM** framework and reporting process
2. **Raise risk awareness** at all levels of the organization
3. Report only **prioritized KRIs** to the board to reduce volume and detail of information
4. Create **dashboard view** of board packet to focus on high risk KRIs

WINTRUST FINANCIAL



CHALLENGES

RESPONSES

1

ERM NOT EFFECTIVELY APPLIED TO IT / IS

- ERM framework existed for broader organization
- Improvement needed for identifying and reporting critical risks

- Developed traceability from operational IT / IS metrics up to ERM framework
- Obtained Committee and Board Level approvals for governance methodology

2

NO IT / IS GOVERNANCE FRAMEWORK IN PLACE

- IT department was focused on operational risk
- InfoSec was recently carved out from IT

- Leveraged the FFIEC Cybersecurity Assessment Tool (CAT) results and framework as a baseline
- Built a matrix of policy requirements for metrics

3

METRICS FOCUSED ON TACTICAL IT PERFORMANCE

- Limited data sources were available
- Little time to show marked improvement

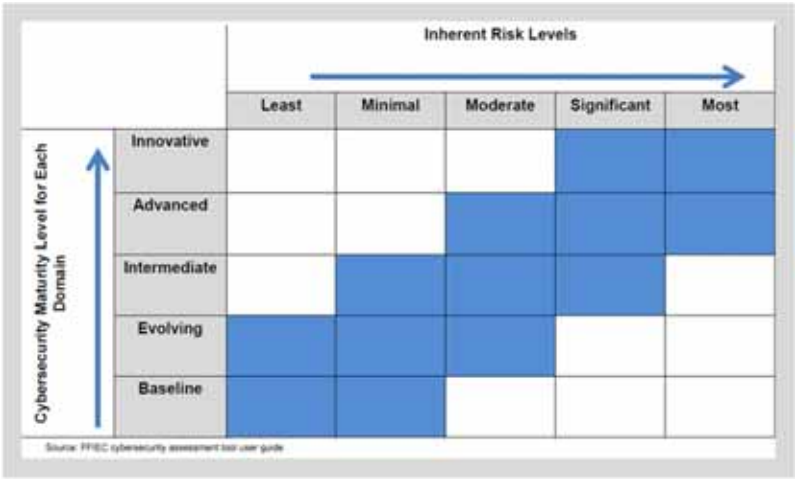
- Identified 15 initial KRIs to align with the ERM model including thresholds and target audience
- Outlined a metrics roadmap of future KRIs to publish in-line with the program's maturity plan

FFIEC CYBERSECURITY ASSESSMENT TOOL (CAT)

- Wintrust completed a risk assessment using the FFIEC CAT to identify which domains and assessment factors carried the most risk
  - Leveraged CAT to establish risk profile
  - Conducted a maturity assessment
  - Metrics were developed to address high risk domains and factors

FFIEC Cybersecurity Assessment Tool

Domain	Assessment Factors
1 Cyber Risk Management & Oversight	• Governance • Risk Management • Resources • Training and Culture
2 Threat Intelligence & Collaboration	• Intelligence Sourcing • Monitoring and Analyzing • Information Sharing
3 Cybersecurity Controls	• Preventative Controls • Detective Controls • Corrective Controls
4 External Dependency Management	• Connections • Relationships Management
5 Cyber Incident Management & Resilience	• Incident Resilience Planning and Strategy • Detection, Response and Mitigation • Escalation and Reporting



DEVELOPED KRI SET BASED ON CAT ASSESSMENT

Multiple views created depending on audience

KRI Tiers
Tier 1: Board Level KRIs
Tier 2: IT/IS Committee Level KRIs
Tier 3: CISO / Management Level KRIs

Presentation format was adopted from the ERM model

Thresholds were established to align with risk appetite

Risk trending built into the presentation

Metrics were organized by CAT domain

Future metrics roadmap created with

Cyber Risk Management & Oversight	Risk Appetite			Jul-17	Jun-17	May-17	Apr-17	Mar-17	Feb-17	Jan-17	Dec-16	Nov-16	Oct-16	Sep-16	Aug-16	KRI TREND
% of Security Awareness Training Completed on Time	> 90%	≥ 89% < 75%	< 75%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	STABLE
Failure Rate % of Mock Phishing Campaign	< 10%	>10% < 15%	>15%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	DECREASING
Threat Intelligence & Collaboration	Risk Appetite			Jul;-17	Jun-17	May-17	Apr-17	Mar-17	Feb-17	Jan-17	Dec-16	Nov-16	Oct-16	Sep-16	Aug-16	KRI TREND
Financial Services (FS-ISAC) Cyber Threat Level	≤ 1	≥2	≥3	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	STABLE
Infocon SANS Storm Center Threat Level	≤ 1	≥2	≥3	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	STABLE
Cybersecurity Controls	Risk Appetite			Jul-17	Jun-17	May-17	Apr-17	Mar-17	Feb-17	Jan-17	Dec-16	Nov-16	Oct-16	Sep-16	Aug-16	KRI TREND
% of Quarterly Access Control Reviews Complete	> 90%	≥ 89% < 75%	< 75%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	INCREASING
% of Level 1 Applications with Provisioning Standards Documented	100%	≥90%	<90%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	INCREASING
Risk Score of Patches Not Applied >90 Days	tbd	tbd	tbd	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	DECREASING
Risk Score of Patches Not Applied >60 Days	tbd	tbd	tbd	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	STABLE
Risk Score of Unsupported Systems	0	tbd	tbd	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	STABLE
Risk Score of Unsupported Applications (Future KRI)	tbd	tbd	tbd	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
% of Open Security Code Findings (Future KRI)	tbd	tbd	tbd	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Third Party Security Management	Risk Appetite			Jul-17	Jun-17	May-17	Apr-17	Mar-17	Feb-17	Jan-17	Dec-16	Nov-16	Oct-16	Sep-16	Aug-16	KRI TREND
% of Third Party Reviews Completed	> 90%	≥ 89% < 75%	< 75%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	INCREASING
# of Third Party Control Requirements Open > 30 days	≤2	>2 <5	≥5	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	STABLE
Cyber Incident Management and Resilience	Risk Appetite			Jul-17	Jun-17	May-17	Apr-17	Mar-17	Feb-17	Jan-17	Dec-16	Nov-16	Oct-16	Sep-16	Aug-16	KRI TREND
# of Open vs Closed Incidents	tbd	tbd	tbd	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	STABLE
% of Devices Impacted by Malware	≤ 1%	>1% <3%	≥3%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	STABLE

QUESTIONS AND ANSWERS?

END OF PRESENTATION

THANK YOU FOR YOUR TIME AND ATTENTION!

IIA CHAPTER CHICAGO | 58TH ANNUAL SEMINAR