



SOA 2018 ERM Symposium

**Keynote Presentation
April 19, 2018**

James Lam

President, James Lam & Associates

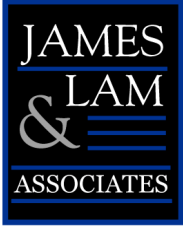
Director and Chair, Risk Oversight Committee, E*TRADE Financial

Director, RiskLens

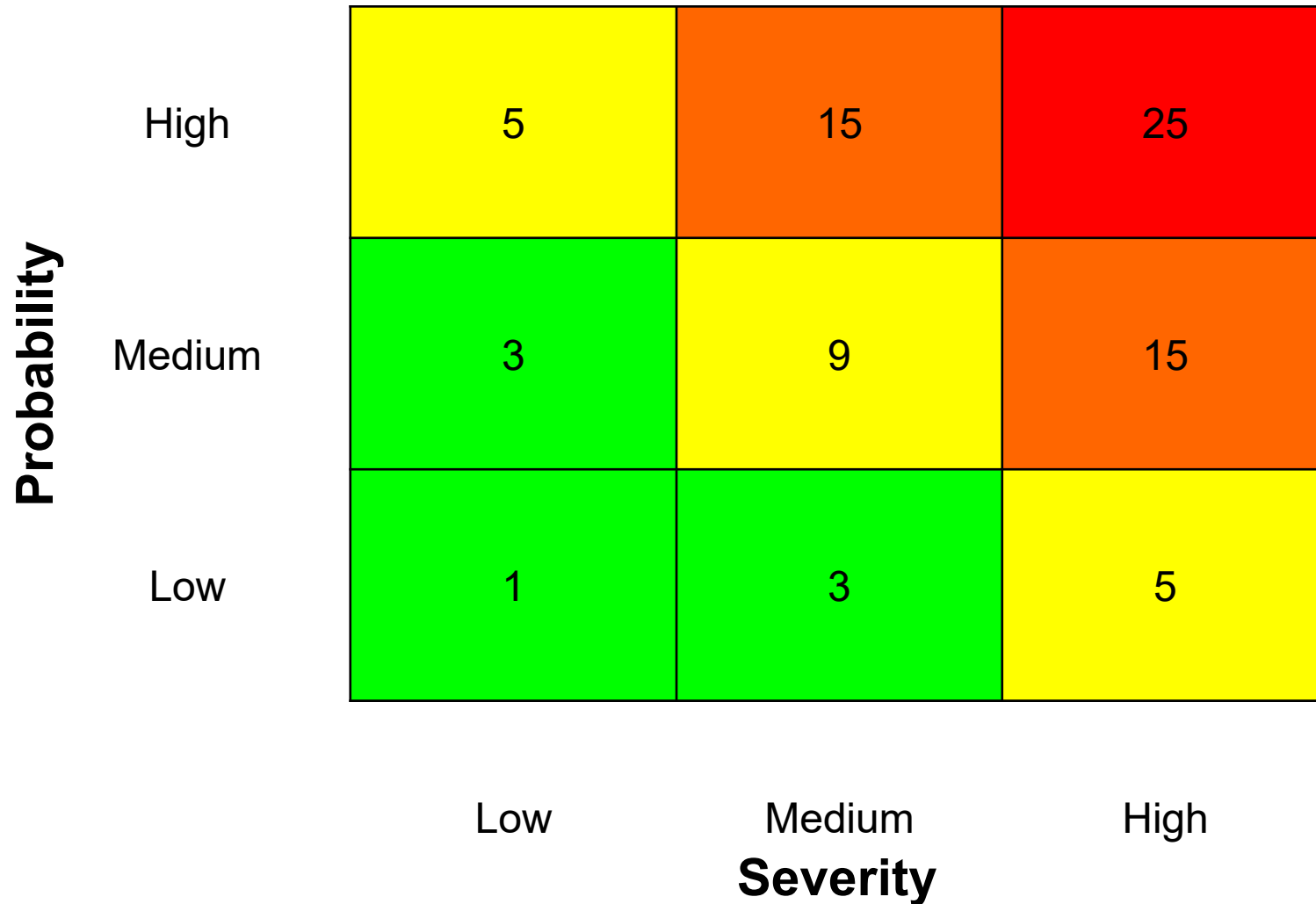


Group question

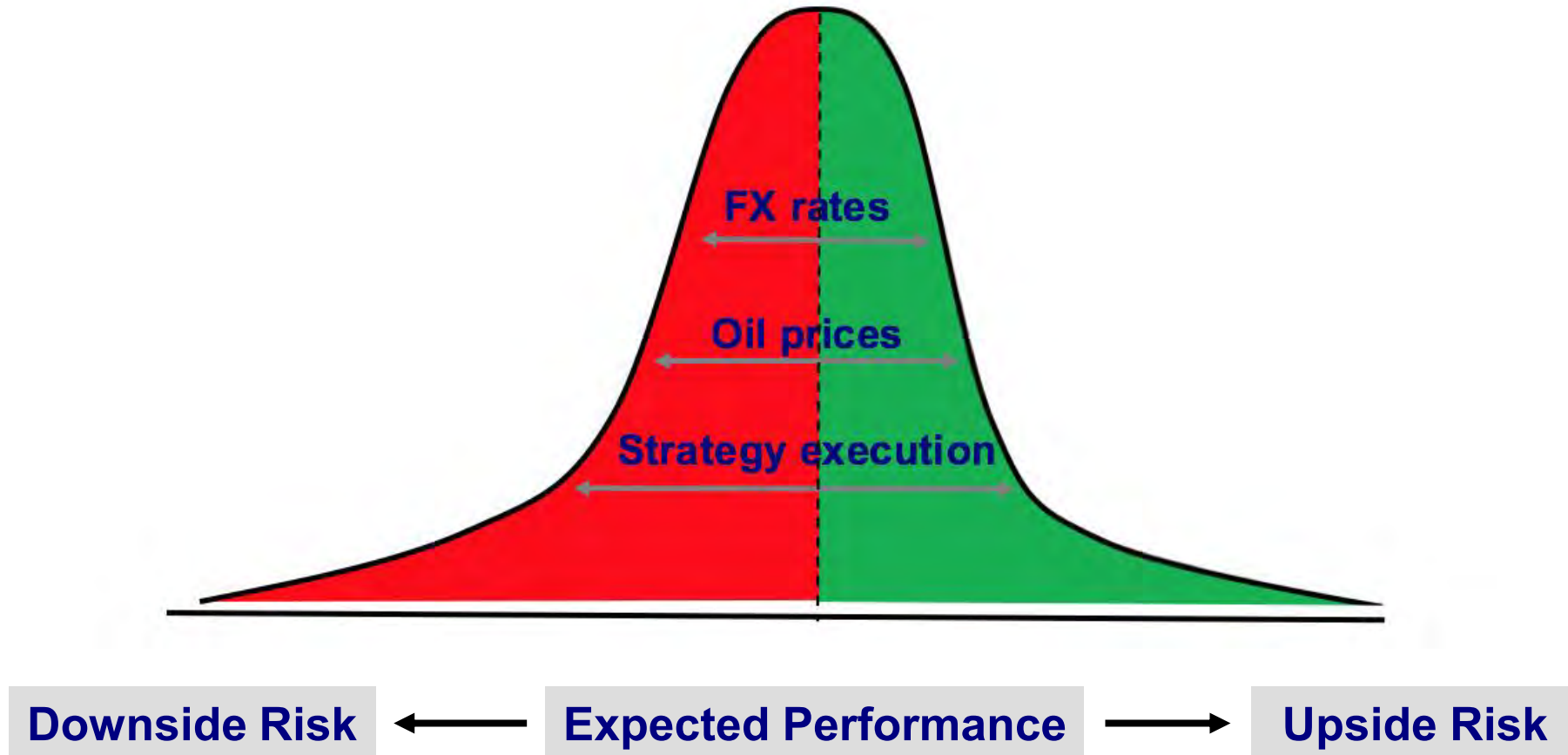
“In your mind’s eye, what is the shape of risk?”



Did you see a heat map or risk assessment?

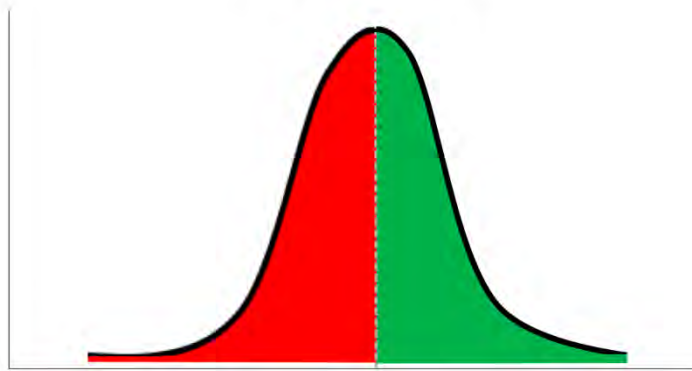


Risk is a bell curve!

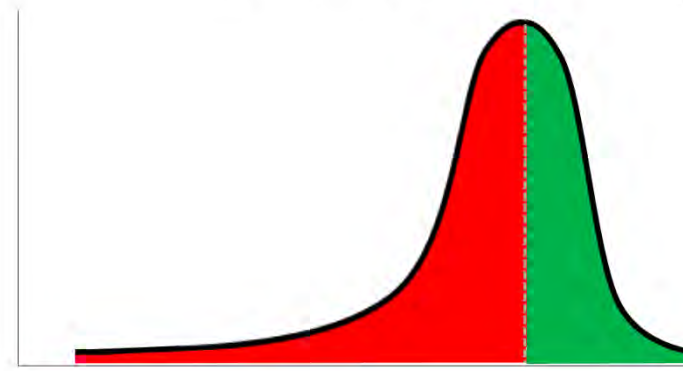


Risks come in different shapes and sizes

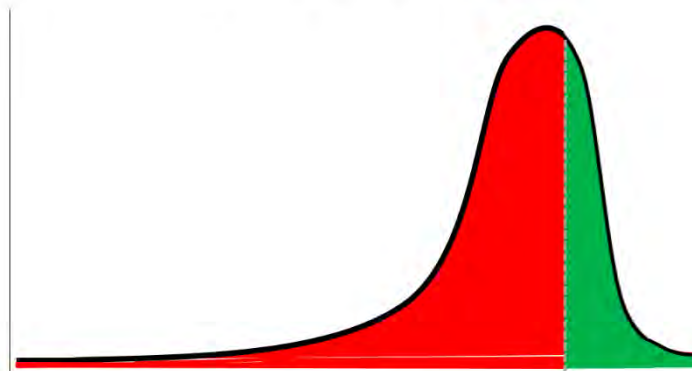
Market Risk



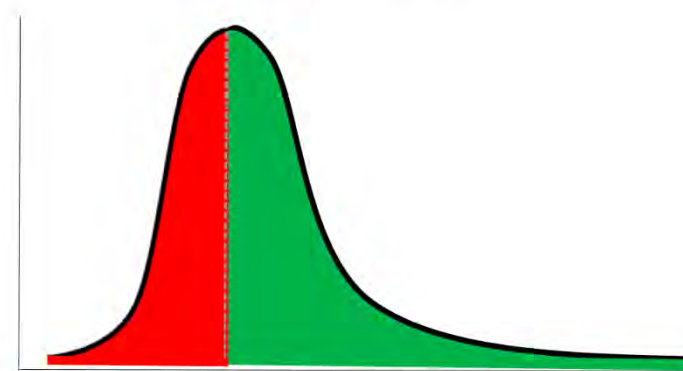
Credit Risk



Operational Risk



Strategic Risk



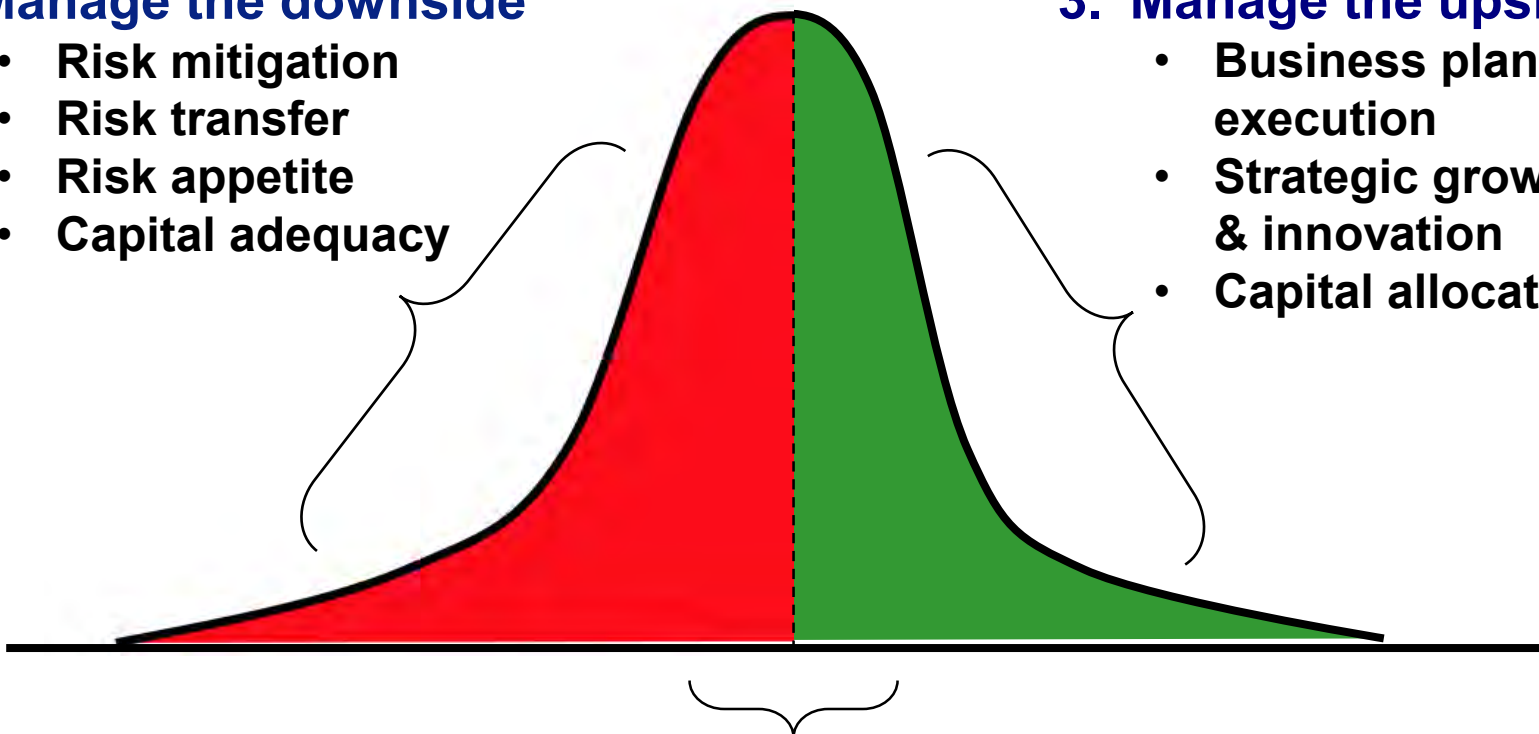
Risk management is about optimizing the bell curve

1. Manage the downside

- Risk mitigation
- Risk transfer
- Risk appetite
- Capital adequacy

3. Manage the upside

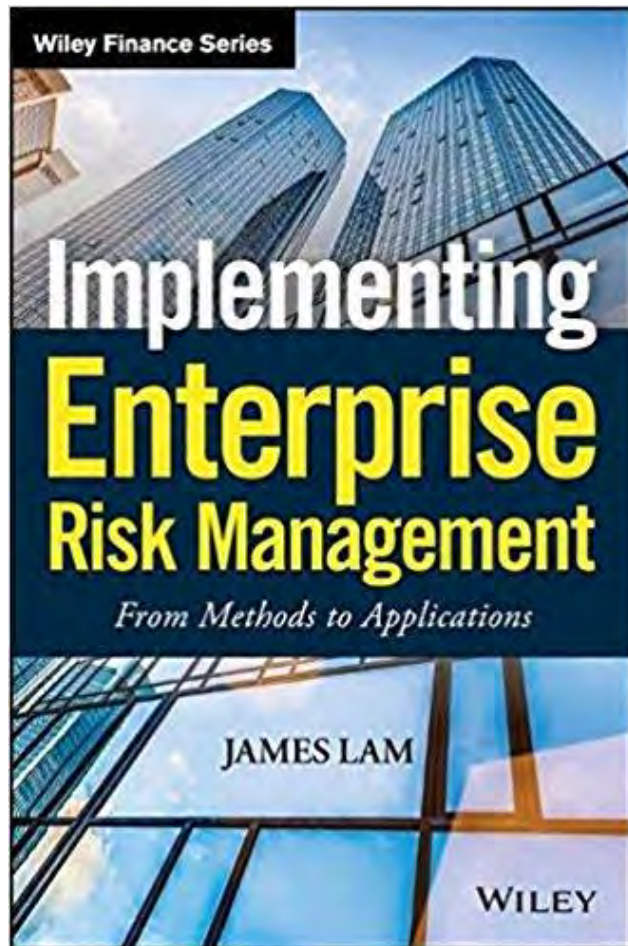
- Business plan execution
- Strategic growth & innovation
- Capital allocation



2. Manage the expected

- Risk acceptance/ avoidance
- Pricing for the cost of risk

ERM should be defined as a value-added function



- **Risk** is a variable that can cause deviation from an expected outcome.
- **Enterprise risk management** is an integrated and continuous process for managing enterprise-wide risks—strategic, financial, operational, compliance, and reputational risks—in order to minimize unexpected performance variance and maximize firm value.



The evolution of ERM

State of ERM

Phase One

**Early 1990s
to mid 2000s**

Major Events and Risks

- Derivatives losses (1994): Orange County, Procter & Gamble, Gibson
- Rogue traders (1994-1995): Barings, Kidder, Daiwa
- Accounting fraud (2000/2001): Enron, WorldCom, Tyco

Key Developments

- Basel I; Group of 30 Report
- VaR models; real-time market risk management
- Sarbanes-Oxley
- Operational risk management

Phase Two

**Mid 2000s to
present**

- Global financial crisis (2008): Lehman, Bear Sterns, AIG
- Energy price volatility; China slowdown, negative interest rates; cyber-attacks

- Basel II; ORSA
- Dodd-Frank
- Stress-testing
- Scenario analysis
- Strategic risk management

Phase Three

**The next 5-10
years**

- Cybersecurity
- Big data, AI, IoT
- Climate change
- Geo-political risks; global terrorism

- Basel III
- SEC Cybersecurity Disclosure
- NIST and ISO 31000
- ENISA; NIS Directive
- Continuous ERM

The E*TRADE story has evolved



- E*TRADE was an early pioneer in the online brokerage industry, having executed the first-ever electronic trade by an individual investor over 30 years ago.
- In 2007, the Company faced the brink of collapse due to sizable and poorly timed investments in mortgages and other asset-backed securities.
- The Company was challenged by large investment losses, intense regulatory scrutiny, activist investor pressure, and weak capital position.
- In 2012, the Company pursued a turnaround plan, including new board members and new management, with a focus on enterprise risk management (ERM).



Key ERM priorities as new E*TRADE Risk Oversight Committee Chairman

1. Establish a strong **ERM agenda** for the Risk Oversight Committee (ROC)
 - Calendar to cover key risks, regulatory requirements, and ERM roadmap
 - Board risk oversight beyond financial and regulatory risks to focus on strategic and operational risks, as well as risk culture
2. Strengthen **independent risk oversight** by formalizing the reporting relationships between the ROC and the Chief Risk Officer and Chief Compliance Officer
3. Enhance the process to review and approve risk policies, with a focus on the **Risk Appetite Statement**
4. Improve the quality and effectiveness of **risk reports** that go to the Board
5. Establish an ERM performance **feedback loop** by linking ex-ante earnings-at-risk analysis and ex-post earnings attribution analysis



CRO Report to the Risk Oversight Committee

February 23, 2018
E*TRADE
Chief Risk Officer (CRO)
Enterprise Risk Management
Committee - Monthly Report

Contents

- CRO Monthly Assessment 3
- New Incidents & Concerns 4
- Emerging Risks & Heightened Concerns 6
- Review of Key Risks by Risk Type 9
- RAS Metric Definitions 28

February Committee Topics

- Interest Rate Risk Update
- Enterprise Risk Management Update
- OptionsHouse Acquisition Update
- Information Security Plan Update
- MAP Extensions Update
- Approve Three Policies
- Approve One Charter

CRO ERM Committee Summary February 23, 2017

CRO MONTHLY ASSESSMENT

Market events during the past month presented significant challenges to the Company's first and second line risk management in the areas of margin and the infrastructure performed well, and despite losses the firm during the extreme market conditions was strong. That said, in weaknesses and brought into relief other improvement

is one example of why E*TRADE's aggregate risk exposure on Security, Data and Operational risks remain high given their volatility expectations. The composite assessment is further mitigated by Legal, Regulatory, Regulatory/Compliance and

entered into a period of elevated volatility, the first meaningful trading the first 24 hours and largely in after-hours trading margin and futures rose to \$8.4 million. Of the \$8.4 million, -volatility exchange \$2 million was from and margin calls were notification between the was excellent, the customer due ber of enhanced d to be ements has now just project track

Risk Type	Status
Information Security Risk	Red
Operational Risk	Red
Data Management Risk	Red
Reputational Risk	Yellow
Strategic Risk	Yellow
Legal Risk	Yellow
Regulatory & Compliance Risk	Yellow
Capital Ratios	Green
Credit Risk	Green
Market Risk	Green
Liquidity Risk	Green
Aggregate - "Elevated"	Yellow

SUMMARY - ELEVATED

ains elevated following increased market volatility, peer interpretations of E*TRADE's retirement advertising

experienced elevated volatility for the first time since plumes increased significantly with the highest levels of During this time, several of E*TRADE's peers an across several of their applications, which generated including high profile articles and social media chatter, any outages, the company can expect heightened and industry pundits should E*TRADE experience

a wide-reaching retirement advertising campaign on feedback has been positive, there are a handful of it is against E*TRADE can expect heightened of the general public as the campaign expands to

vice, and Corporate Communications teams concerns.

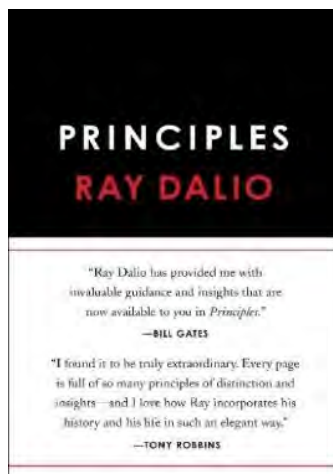
Dashboard - Reputational Risk Metrics

Metric	Nov 17	Dec 17	Jan 18
Negative Social Servicing Comments	182	48	53
Public	6217	6217	6217
Platform Customer Satisfaction	87.8%	87.8%	82.9%

Active mentions were both Bloomberg articles related to well. Social media mentions remain light.

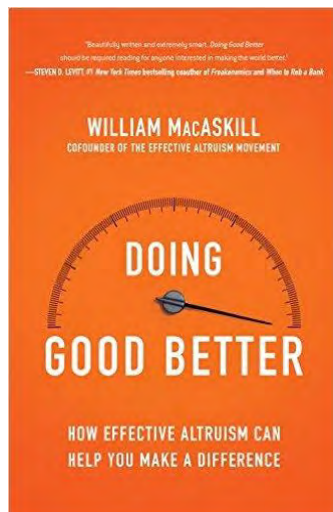
- Executive Summary
- New Losses & Events
- Follow-up on Prior Losses & Events
- Emerging Risks
- Key Risk Reviews and Metrics vs. Risk Tolerances
- Progress against the ERM Roadmap
- Terms and Definitions

The importance of feedback loops is widely recognized across disciplines



Ray Dalio, Founder of Bridgewater Associates

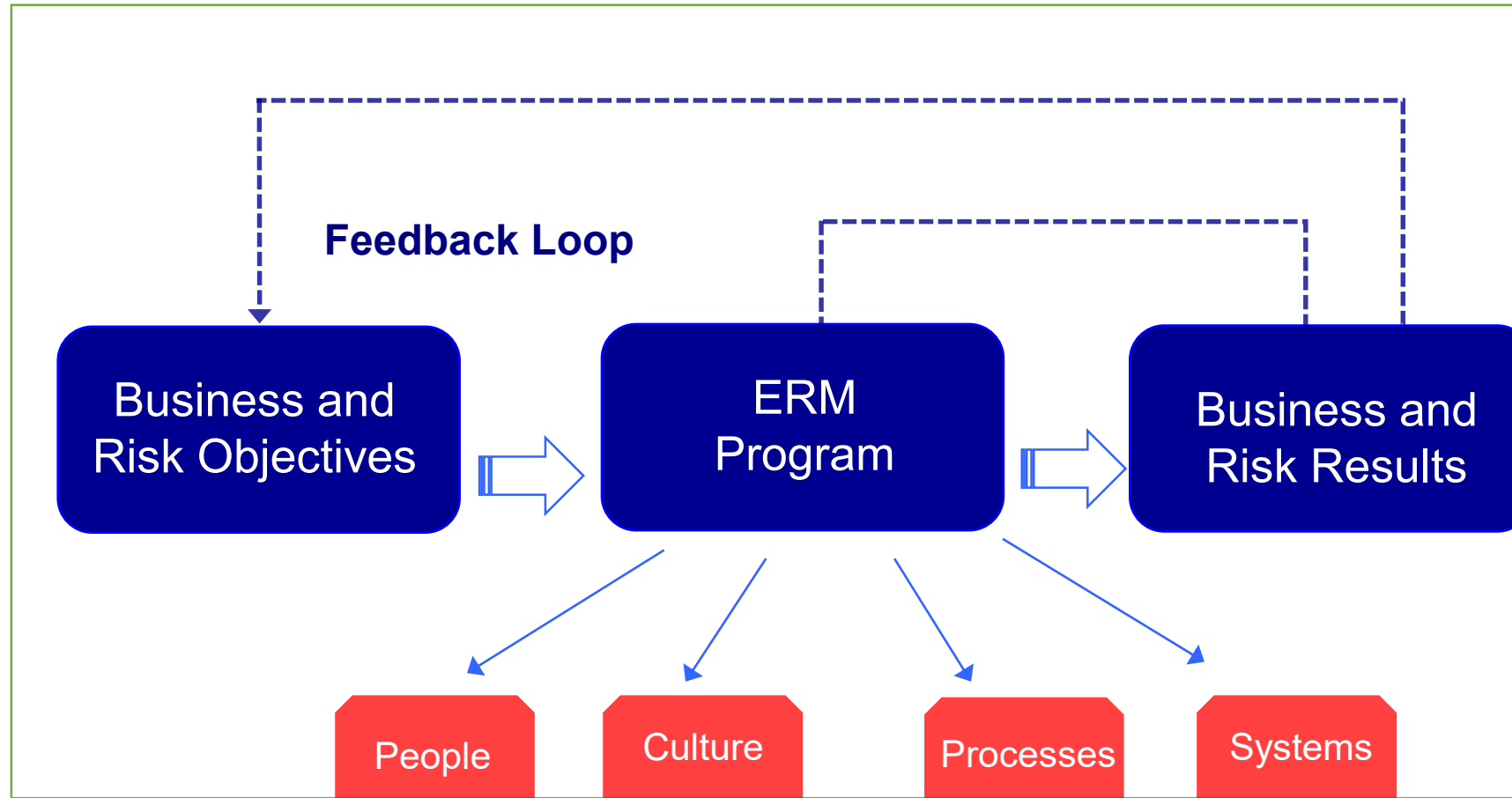
- Founded in 1975; based in Westport, CT
- Over \$150 billion in assets under management
- Recognized for innovation and performance; unique culture of continuous feedback and transparency
- Apply feedback loops to make changes in staff and organizational culture



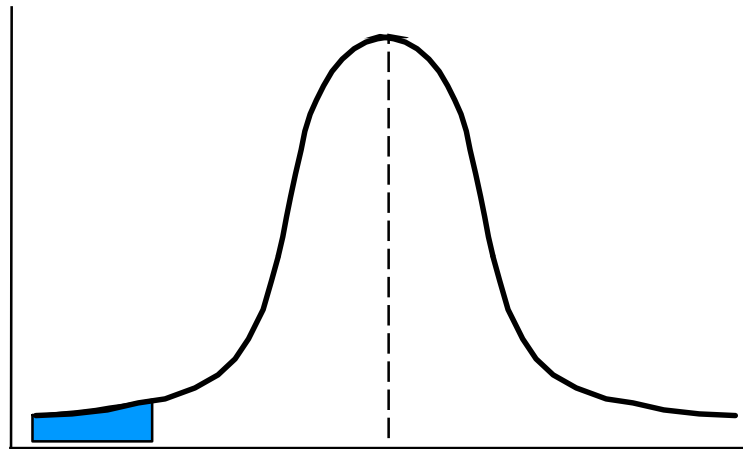
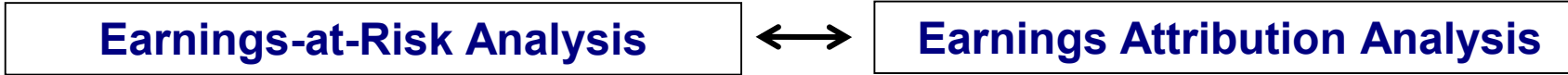
William MacAskill, Co-Founder, Effective Altruism

- A new scientific approach to determine the most effective ways to direct charity and improve the world
- Two case studies: (1) PlayPump, a water pump designed as a merry-go-round, and (2) deworming, a cost-effective method to improve school performance
- Use quality-adjusted life years (QALY) saved per dollar to allocate limited resources

ERM performance feedback loop



Key question: how do you know if risk management is working effectively?



Worst Case EPS = (\$1.00) Expected EPS = \$3.00

- | | |
|---------------------|---------------|
| 1. Business Plan: | \$2.00 |
| 2. Interest Rates: | \$1.00 |
| 3. Oil Price: | \$0.50 |
| 4. Key Initiatives: | \$0.30 |
| 5. Expense Control: | <u>\$0.20</u> |
| | \$4.00 |

Expected EPS :	\$3.00
Actual EPS:	<u>\$1.00</u>
Difference:	\$2.00
Business Plan:	\$1.00
Interest Rates:	\$0.50
Key Initiatives:	\$0.10
Unforeseen Factors:	<u>\$0.40</u>
	\$2.00

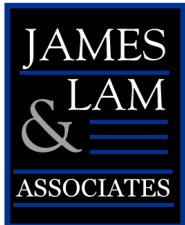
Key Questions:

1. Did we identify the key risk factors?
2. Were our EPS sensitivity analyses accurate?
3. Did risk management impact our risk/return positively?



The “Lam Report” (illustrative data)

Earnings Sensitivity		Downside	2018 Budget	Upside	2018 Earnings Sensitivity (\$M)		
Business Drivers	New Assets (\$B)	\$9.0	\$8.0 \$9.0	\$12.0	(\$30)	\$35	
	Customer Attrition (%)	10.0%	8.0% 6.0%	5.0%	(\$45)	\$45	
	Operating Costs (\$B)	\$4.0	\$5.0 \$6.0	\$8.0	(\$10)	\$10	
	Revenue / Growth (\$B)	\$1.5	\$2.0 \$3.0	\$4.5	(\$5)	\$5	
	Balance Sheet Size (\$B)	\$60.0	\$63.0 \$65.0	\$70.0	(\$25)	\$25	
Credit	Default Rate (%)	4.0%	3.6% 3.0%	2.0%	(\$40)	\$40	
	Severity (%)	35.0%	30.0% 25.0%	15.0%	(\$30)	\$30	
Pre-Tax Income (Downside / Upside)			● 2018 Budget ● 2017 Actual		\$315 M	\$500 M	\$690 M



E*TRADE Financial

Performance	December 2012	December 2017
Stock Price	\$9 per share \$2.7 billion market cap	\$50 per share \$13.2 billion market cap
Net Income	\$(113) million	\$614 million
Capital Adequacy	5.5% Tier 1 Leverage	7.6% Tier 1 Leverage
Debt Rating	S&P: B- Moody's: B2	S&P: BBB Moody's: Baa3
Regulatory	Under MOUs from the OCC and the Federal Reserve	MOUs lifted by the OCC in Q1 2015 and the Fed in Q2 2015

The upside and downside of cybersecurity



“The best customer service is if the customer doesn’t need to call you....it just works.”

- Jeff Bezos



“I do think..[cyber]..is the number one problem with mankind”

- Warren Buffet

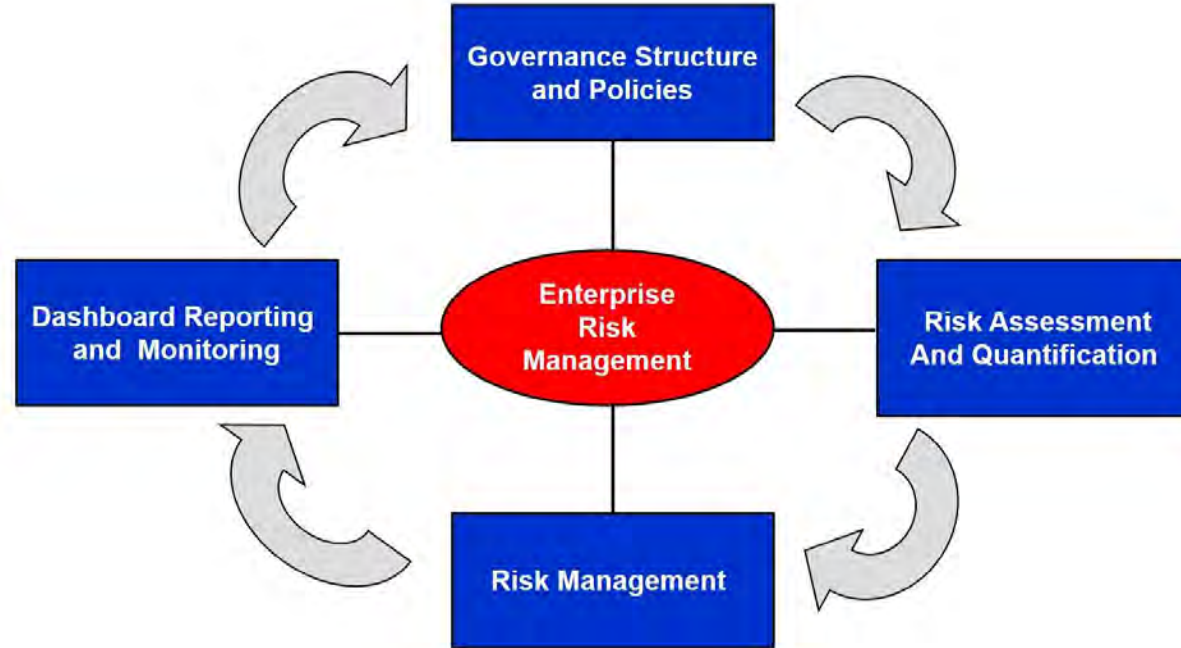


Current approaches to cybersecurity are failing

- **90%** of value of S&P500 consists of IP and intangibles
- **\$75B** spent annually on security
- **80%** of large enterprises are breached
- **146** days average detection time
- **\$2.1T** cybercrime cost in 2019

Cyber offense has a structural advantage over defense.

ERM vs. NIST Framework

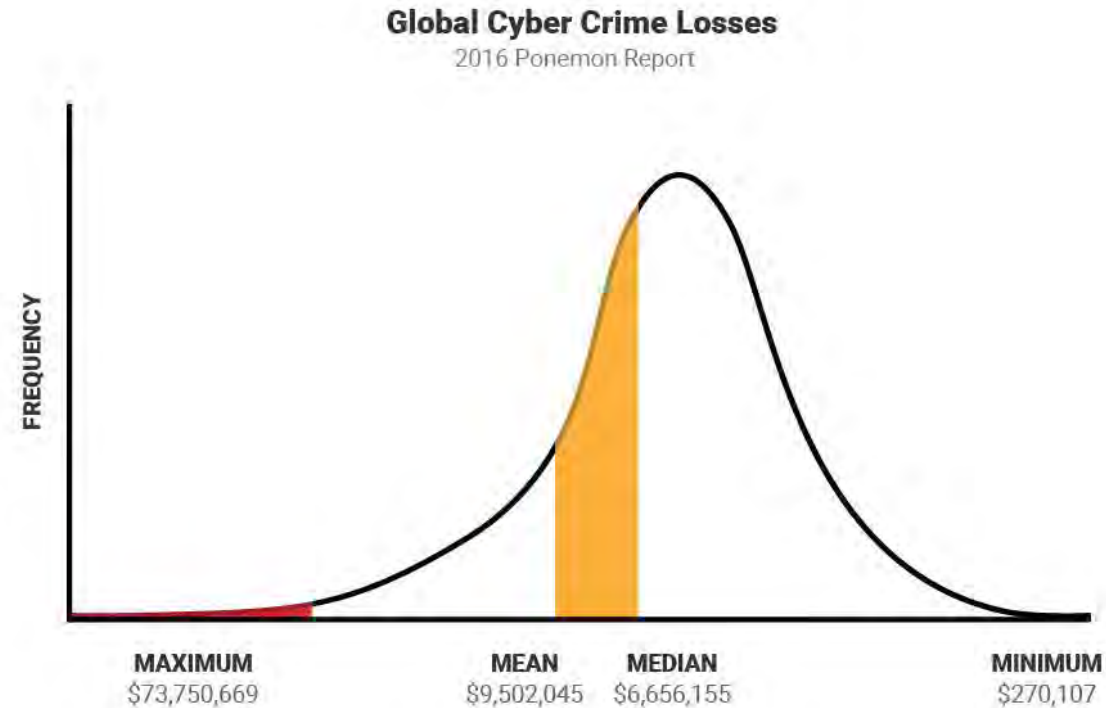


What is missing in NIST?

- Cyber risk governance
- Cybersecurity risk policy and strategy
- Cyber risk quantification
- Risk appetite tolerance
- Reporting and performance feedback



Quantitative Drivers of Potential Loss



Value-at-Risk (VaR) Drivers for Any Risk:

$$\boxed{\text{Exposure}} \times \boxed{\text{Probability}} \times \boxed{\text{Severity}} \times \boxed{\text{Correlation}} = \boxed{\text{Potential Loss}}$$



Risk drivers for market, credit, and cyber risk

Component	Market Risk	Credit Risk	Cyber Risk
Exposure	Investment portfolio	Loan portfolio	Digital assets portfolio
Probability	Probability of loss or gain <ul style="list-style-type: none"> Market price volatility 	Probability of default <ul style="list-style-type: none"> Economic conditions Credit ratings 	Probability of breach <ul style="list-style-type: none"> Threat vectors Preventative controls
Severity	Holding period <ul style="list-style-type: none"> Market liquidity of investments 	Loss in the event of default <ul style="list-style-type: none"> Collateral rights Bankruptcy rights 	Loss in the event of breach <ul style="list-style-type: none"> Dwell time Resolution time Detective, mitigation, and proactive controls
Correlation	Price correlations <ul style="list-style-type: none"> Asset allocation Position concentrations 	Default correlations <ul style="list-style-type: none"> Loan concentrations Country/industry diversification 	Threat/control correlations <ul style="list-style-type: none"> Cyber attack patterns Central points of failure: IT infrastructure, supply chain



Example: cybersecurity metrics

Threat Environment

- E-ISAC Cyber Threat Trend
- NCFTA Cyber Fraud Threat
- Global Computer Virus & Spyware Activity

General Information Security

- Number of systems and applications, including those deemed critical
- Value of digital assets, including “crown jewels”

3rd Party Vendor Risk

- Number of high risk, critical 3rd parties
- Critical 3rd parties average and range of security ratings

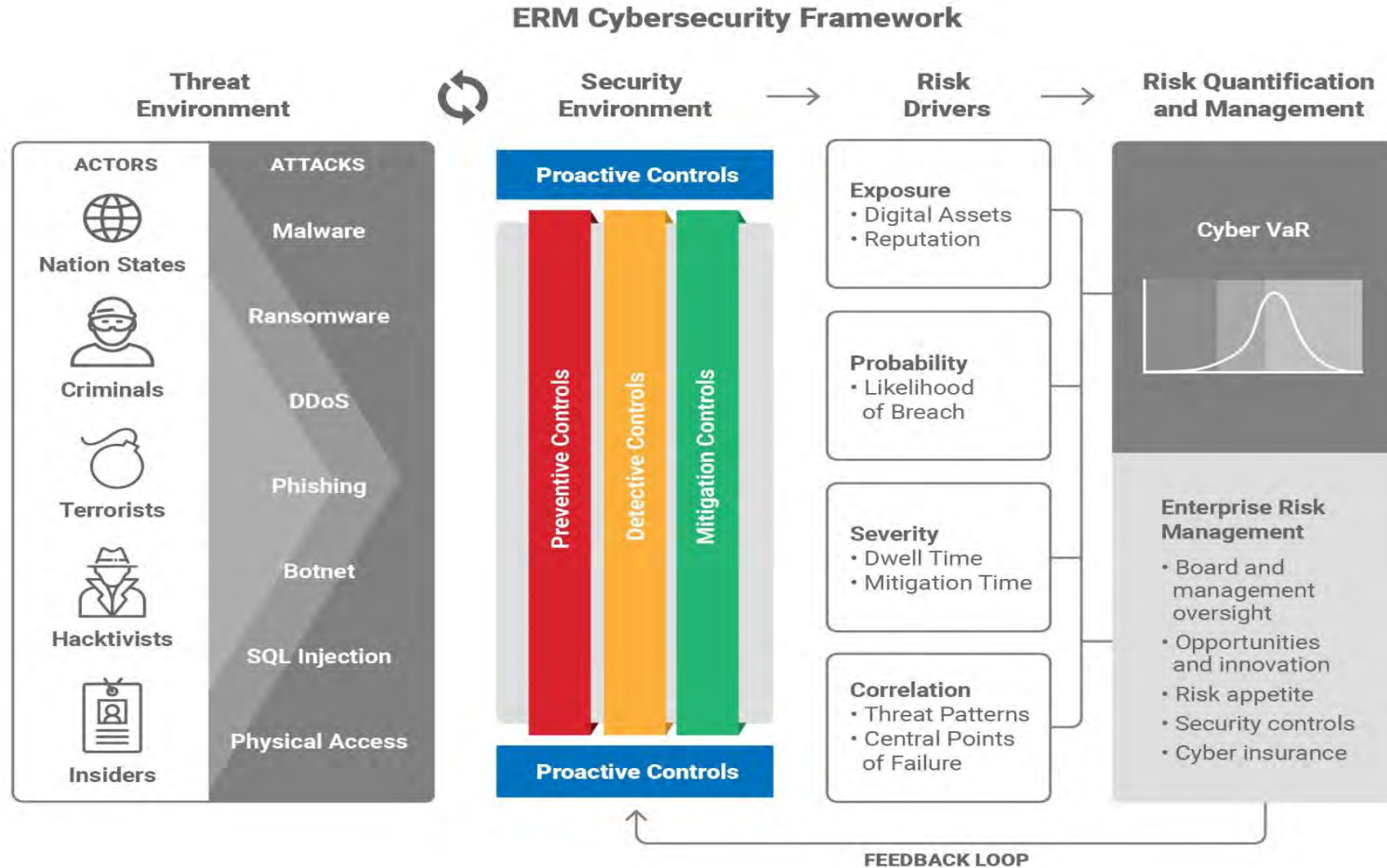
Key Controls

- Enterprise-wide patches deployed within SLA
- Average time to close a cyber case (days)
- % system downtime; time to recover
- Mission critical applications with a tested disaster recovery solution
- Percent of key controls rated below adequate

Program Effectiveness

- Company security rating
- Average time to detect (dwell time)
- Average time to remediate
- Unresolved critical Pentest findings
- Open Audit issues
- Open Regulatory Findings (MRAs)
- NIST program maturity assessment
- Performance of table-top exercises and third-party testing

Integrating Cyber Risk into ERM





Key Takeaways

- 1. Visualize, quantify, and optimize bell curve**
- 2. Board risk oversight should focus on ERM fundamentals: independent oversight, risk appetite, and risk reporting**
- 3. Effective cybersecurity requires better risk quantification and ERM integration**
- 4. Beware of black swans and grey rhinos: invest in preparedness and resilience**
- 5. Establish a performance feedback loop for ERM**



Key Success Factors as a Risk Professional: My Top 5 Lessons Learned

- Lesson #1: Establish clear and tangible goals
- Lesson #2: Develop a “model T” skills set and a branding strategy
- Lesson #3: Develop strong communication skills
- Lesson #4: Learn to play the corporate game
- Lesson #5: Focus on usefulness, not precision