

# NISTIR 8286 Integrating Cybersecurity & Enterprise Risk Management

March 15, 2021

---

**INNOVATE. TRANSFORM. SUCCEED**

Adapt to the new business reality.



# WELCOME

## Introductions – Speaker Profile



### Rebecca Nilson, CPA, CIA, CRMA

**Director | Protiviti Nashville**

**Internal Audit & Financial Advisory Services – ERM Enterprise Risk Management**

#### **Institute of Internal Auditors**

- Board Member Institute of Internal Auditors, Nashville
- 2022 International Conference Co-Chair
- Accredited in Quality Assessment and Validation

**Healthcare Financial Management Association (HFMA), Member**

**Association of Healthcare Internal Auditors (AHIA), Member**

**Northwestern University – Compliance and Enforcement Courses, Guest Lecturer**

[Rebecca Nilson, CPA, CIA, CRMA](#)



# WELCOME

## Introductions – Speaker Profile



### George Quinlan, CISA, CISM, CRISC, CDPSE, Open FAIR

Senior Manager | Protiviti Chicago  
Security Program & Strategy – Cyber Risk Quantification

FAIR Institute – Member, Chicago Chapter

ISACA Chicago Chapter

- Events Committee – Board of Directors
- Certification Review Course Instructor (CISA, CISM, CRISC)

<https://www.youracclaim.com/users/george.quinlan/badges>

[George Quinlan, CISA, CISM, CRISC, CDPSE, Open FAIR](#)



# AGENDA

01

What is NISTIR 8286?

02

What is Enterprise Risk Management vs IT / Cyber / I&T risk management?

03

Why was NISTIR8286 developed?  
What concerns does it address?

04

What is the proposed solution?

NISTIR 8286

## Integrating Cybersecurity and Enterprise Risk Management (ERM)

Kevin Stine  
Stephen Quinn  
Greg Witte  
R. K. Gardner

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.IR.8286>

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

## WHAT IS NISTIR 8286?

- ✓ Enterprise Risk Maturity continuum
- ✓ Clear alignment with objectives

# NISTIR 8286 – PUBLISHED OCTOBER 2020

Intent is to improve the inputs and standardization of cybersecurity risks to Enterprise Risk Management (ERM) to help effectively communicate cybersecurity risks to Senior Leadership and the Board.

- Identifies a broader way to view of cybersecurity risk including areas such as strategic risk, credit, operational, reporting and others across all levels of the organization
- Suggests standard methodologies and frameworks to assess risks such as NIST CSF standards + Open FAIR
- Quantifying risk in business terms, dollars, along with a risk register is critical for board level ERM reporting.
- Cybersecurity risks can be better managed in terms of the business context & mission as it correlates to the organization's strategy or goals.

NISTIR 8286

## Integrating Cybersecurity and Enterprise Risk Management (ERM)

Kevin Stine  
Stephen Quinn  
Greg Witte  
R. K. Gardner

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.IR.8286>

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

Source: <https://csrc.nist.gov/publications/detail/nistir/8286/final>



# ENTERPRISE RISK MATURITY CONTINUUM



Board, CFO, ERM, CIO

## CLEAR ALIGNMENT WITH OBJECTIVES

Aligning various types of cybersecurity risk with enterprise objectives will help enable subsequent aggregation, normalization, and prioritization.



### Strategic

- Risks related to the implementation of a new service offering; cybersecurity issues that might impact an upcoming federal agency merger or private sector acquisition



### Operations

- Cybersecurity issues regarding existing operational systems, such as a ransomware attack that disables a manufacturing line; business continuity/disaster recovery issues



### Reporting

- Cybersecurity risks regarding the availability, integrity, and confidentiality of accounting or other financial management systems



### Compliance

- Cybersecurity risks where a negative event might result in a failure to meet a contractual service agreement or in a regulatory penalty or fine



# LINKING TO MISSION, STRATEGY AND GOALS

## FYXX Operating Goals

- Employee Turnover Rate; Employee Career Development Plan; Employee Wellness
- Patient Safety Index; Inpatient Satisfaction; Ambulatory Satisfaction
- New Patients; Inpatient Volume; Access new patients
- Operating Income; Surgical Volume; Externally Funded



## Strategic Plan 1-3 Years

- Expansion • Improve Costs Metrics • Reposition Core Operations • Service Line Growth • Referral Network Expansion • Recruitment and Retention of High-Performing, Diverse Talent • Mergers and Acquisitions • System Integration • Improve Quality Outcomes • Improve Patient Experience

## Actionable Top Risks Areas

### High Quality, High Care

- Safety (Patient, Visitors, Staff) • Department Climate & Culture • Joint Commission Preparedness
- Business Continuity • Facility Safety • Violence, External to patient units or clinics • Exposure to Regulatory Audit • Drug Diversion
- Disasters: Medication or Supply Shortage • **Cybersecurity** • **IT Failures**

### Rate Pressure

- Unfavorable Contracts
- Inability to Meet Financial Goals
- Flat / Declining Payer Reimbursement
- Claims Submission Documentation & Support

### Patient Shift

Inpatient to Outpatient

### Changing Business Model

- Cybersecurity
- Data Access

### Health Equity

### Increase Costs

340b Program / Drug costs

### Expanding Networks

- Affordable Care Act (ACA)
- In-network agreements

### Workforce Shortage

- Low Staff Engagement
- Manager Effectiveness
- Misaligned Strategic Initiatives
- Not Continuously Investing in Staff Training / Development
- Innovation

### Precision Medicine

- Research Regulatory / Compliance
- Research Clinical Trials Billing

### Mergers and Acquisitions

- Organizational alignment
- Merger/Acquisition Synergies
- Mergers and Acquisitions/Market Consolidation

# What is ERM Anyhow?

- ✓ Risk Management Frameworks
- ✓ Common ERM Implementation Challenges
- ✓ Illustration of ERM Governance and Communication
- ✓ ERM journey continuum

# WHAT IS ERM ?

Every organization is trying to achieve its mission. This usually involves creating a strategic plan that defines objectives. Enterprise risk can be defined as the ***degree of uncertainty*** - both positive (opportunities) and negative (threats) - ***in achieving objectives***.

ERM includes the process of identifying, evaluating and reporting on risks relative to an organization's objectives, so that the plan and ***objectives are achieved more often*** than without this discipline and activity.



## Through experience, we know:

- ERM does not need to be complicated or over-engineered to be successful.
- There is no one-size-fits-all approach to ERM.

## Common criticisms of ERM:

- Its processes and outputs are not engaging or valuable to management.
- ERM can become a siloed, administrative process.

## POLLING QUESTION #1

### Does your organization have an Enterprise Risk Management (ERM) program?



Yes, we have a robust ERM program



Yes, but the ERM program seems to be a check the box task



We are developing a program



HUH? ERM Program?

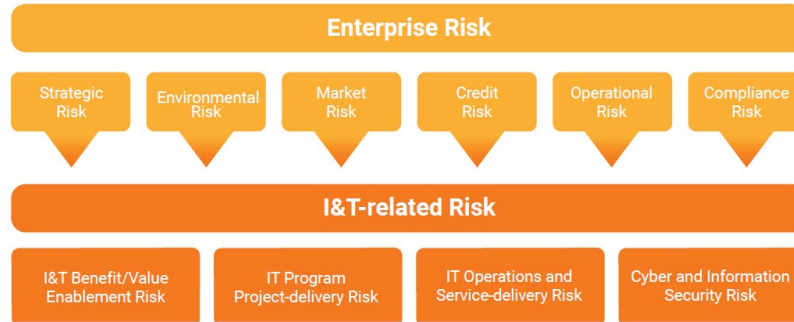


# RISK MANAGEMENT FRAMEWORKS

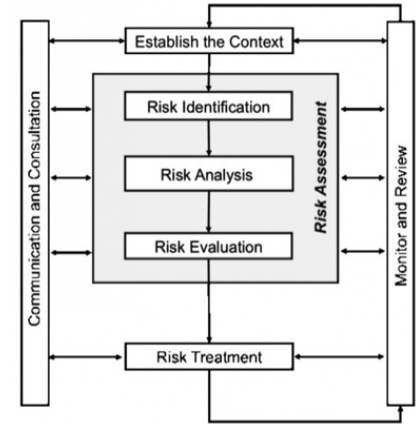
COSO Cube (ERM)



ISACA IT Risk Framework v2.0 (Cobit 5)



ISO31000 Risk Mgmt. Process



**NISTIR 8286  
ERM RISK**

Cybersecurity

Financial

Legal

Legislative

Operational

Privacy

Reputational

Safety

Strategic

Supply Chain

# COMMON ERM IMPLEMENTATION CHALLENGES



Through experience, we have identified some key challenges that need to be managed when implementing an ERM program.

- Misalignment between ERM Program owners and stakeholders on value expectations and scope

- Insufficient planning, leading to risk assessment results that are not actionable

- Excessive focus on risk assessment vs risk management activities

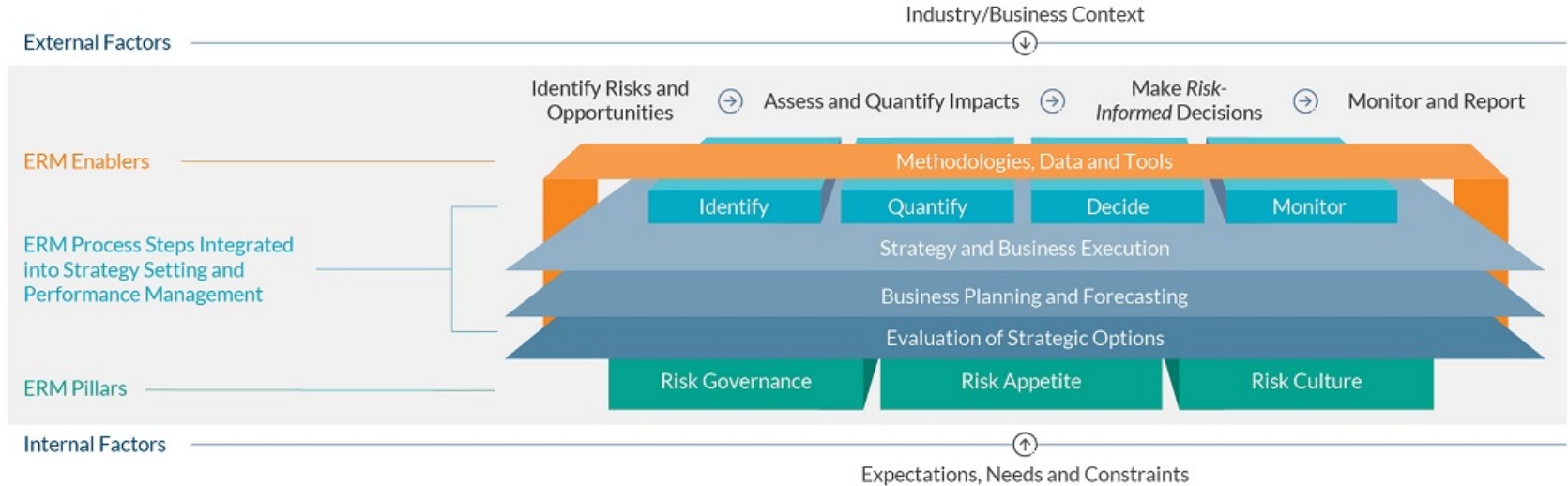
- Adoption of overly complicated methodologies and frameworks

- Not linking the ERM Program to business objectives

- Duplication of effort between the ERM Program and other assurance providers

- Insufficient dedicated 'ERM' resources compared to the anticipated output

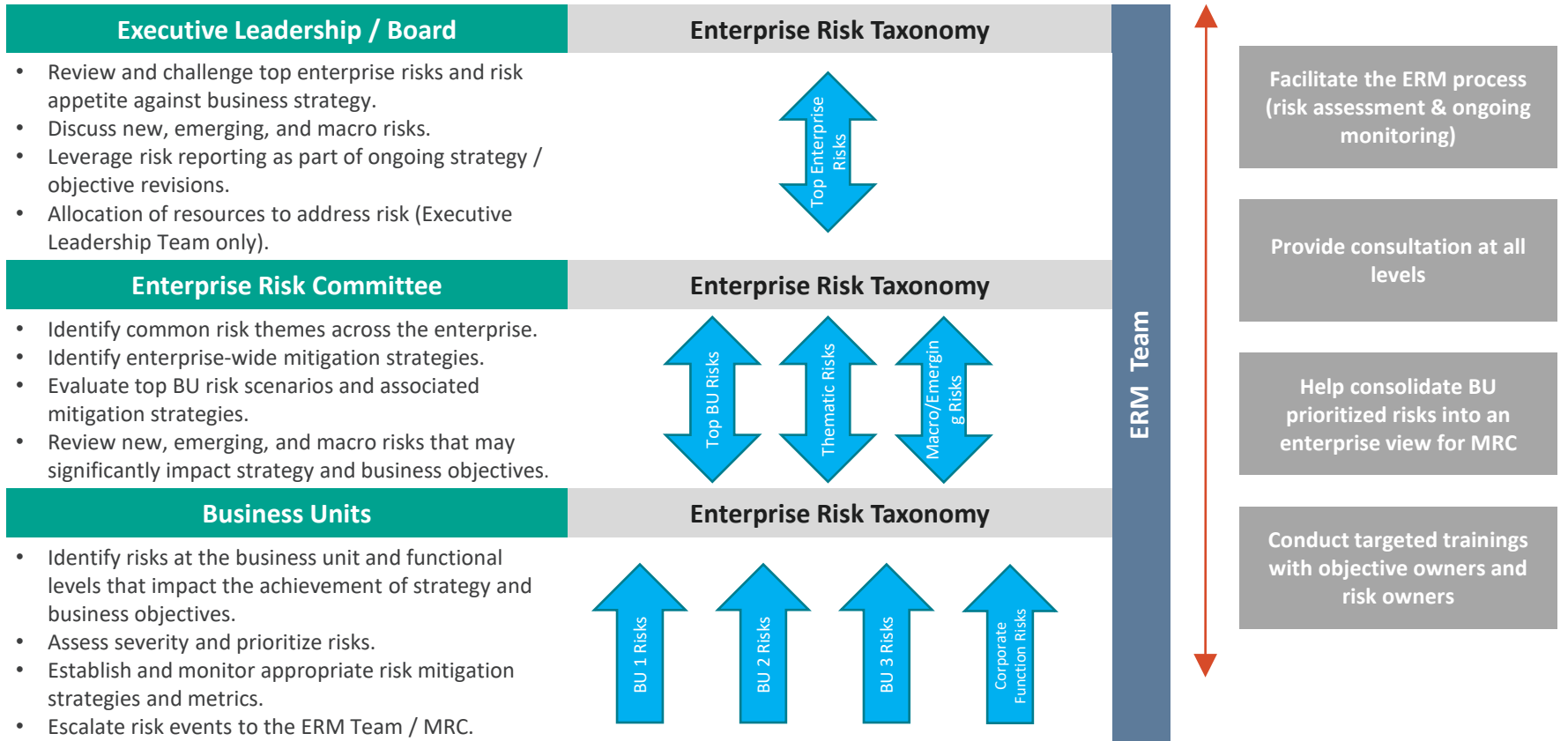
# RISK INFORMED APPROACH



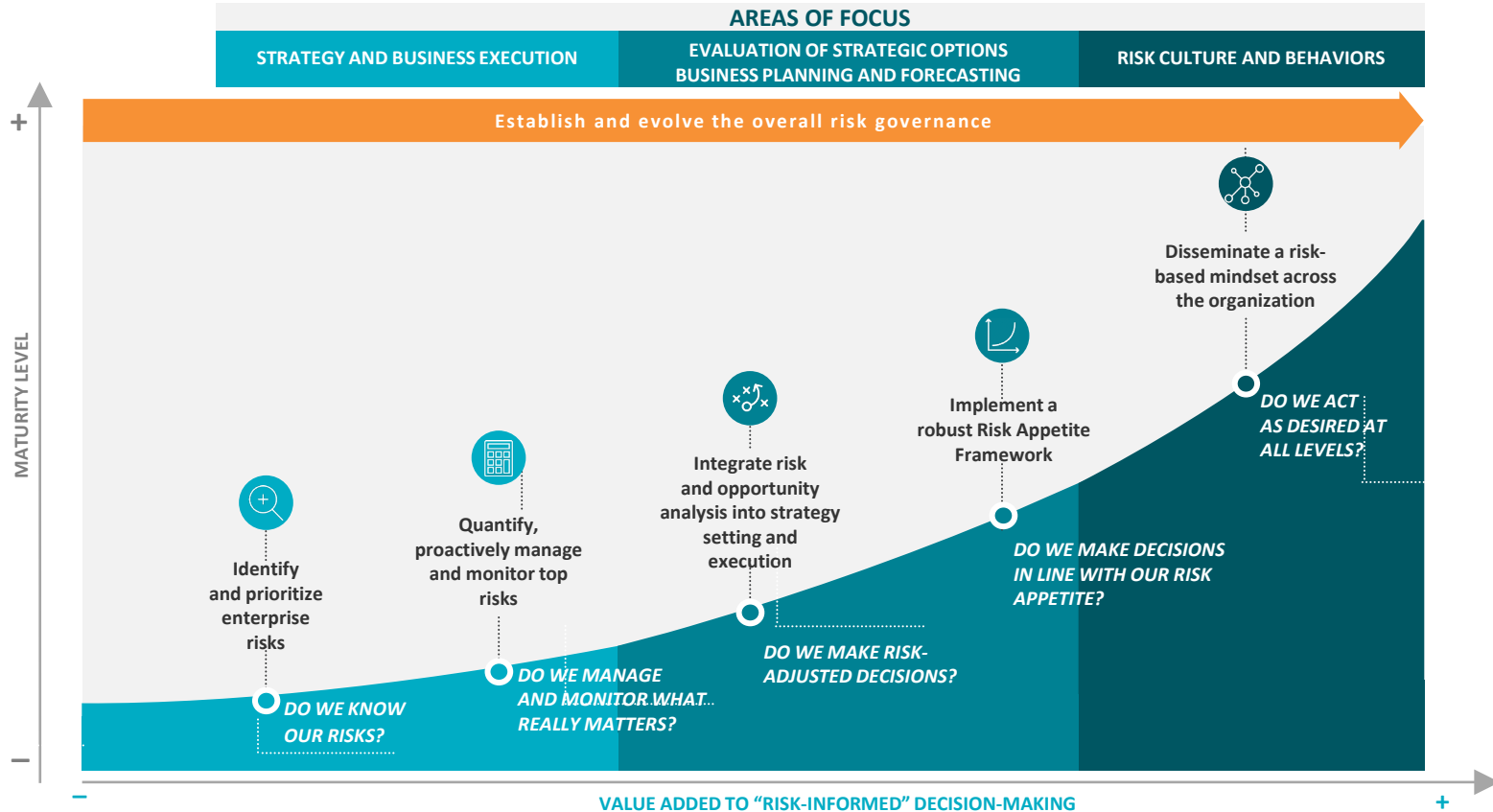
ERM RISK INFORMED APPROACH			
Balanced	Strategic	Integrated	Customized
Measures both risks and opportunities	Considers the impact of risk on strategy and performance	Is integrated with strategy setting, planning and business execution	Reflects organizational business needs, expectations and cultural attributes

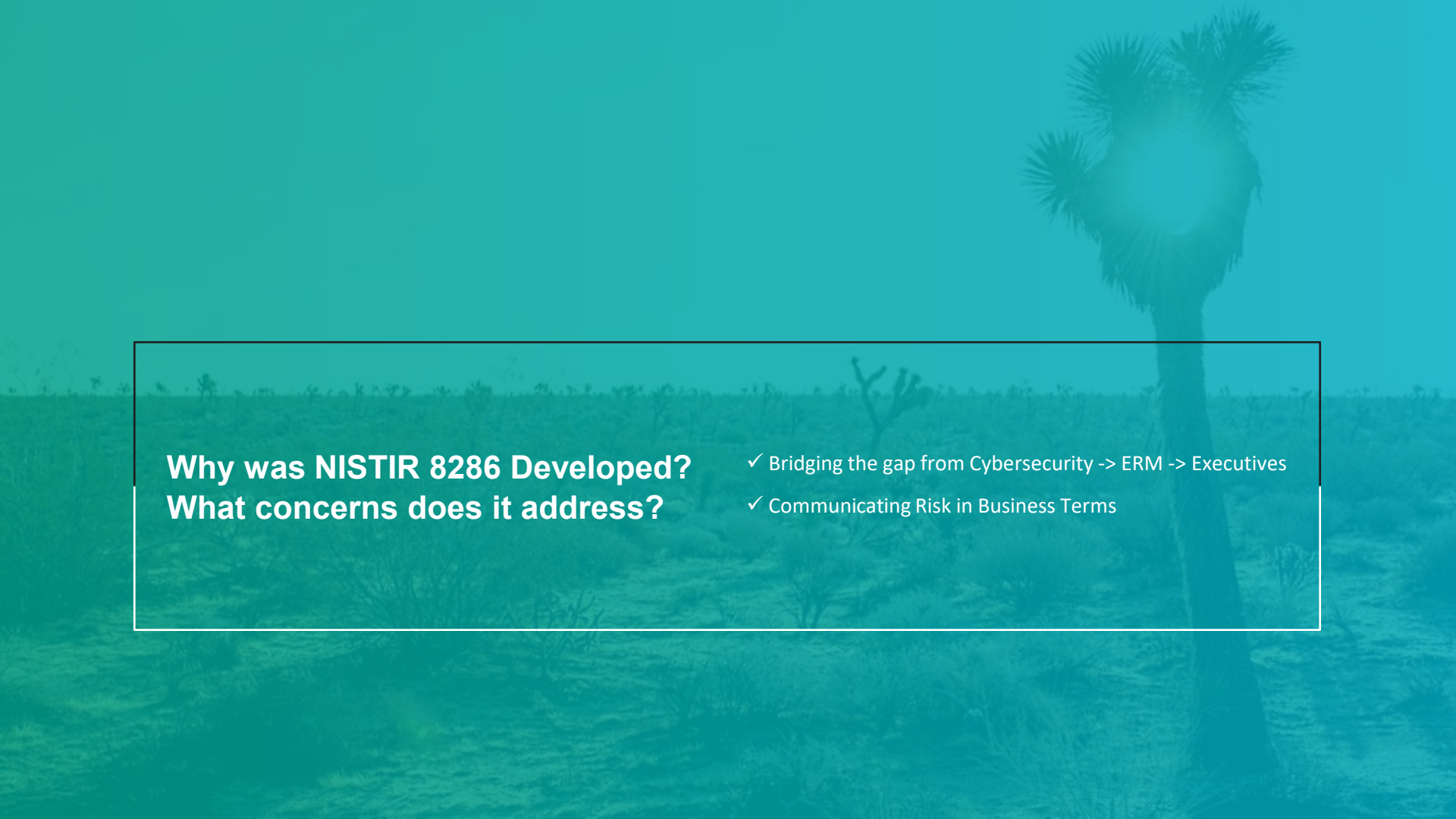


# ILLUSTRATION OF ERM GOVERNANCE AND COMMUNICATION



# THE ERM JOURNEY CONTINUUM





**Why was NISTIR 8286 Developed?  
What concerns does it address?**

- ✓ Bridging the gap from Cybersecurity -> ERM -> Executives
- ✓ Communicating Risk in Business Terms

# BRIDGING THE GAP FROM CYBERSECURITY -> ERM -> EXECUTIVES

How can we communicate to executives in terms they will understand, and help them better understand cybersecurity risks?



## CYBERSECURITY DOESN'T COMMUNICATE TO ERM VERY WELL

Have you ever felt like someone doesn't understand the message you're trying to convey about cyber risks?



- Most enterprises do not communicate their cybersecurity risk guidance or risk responses in consistent, repeatable ways.



- Cybersecurity risks should be documented and tracked in written cybersecurity risk registers that are consistent with the organization's ERM program guidance.



- Methods such as quantifying cybersecurity risk in dollars and aggregating cybersecurity risks are largely ad hoc and are sometimes not performed with the same rigor as methods for quantifying other types of risk within the enterprise.

In addition to widely using cybersecurity risk registers, improving the risk measurement and analysis methods used in CSRM would boost the quality of the risk information provided to ERM. In turn, this practice would promote better management of cybersecurity at the enterprise level and support the enterprise's objectives.

# COMPLIANCE ≠ RISK






Being fully compliant does not mean you are fully secured

## Qualitative Checklists & Frameworks

**NIST**



## Semi-quantitative controls questionnaire

	=	Very Low	=	1
		Low		2
		Moderate		3
		High		4
		Very High		5

The way most organizations measure risk today fails to quantify information and operational risk in terms that the business can understand and use.

# QUANTIFYING CYBERSECURITY RISK IN FINANCIAL TERMS

	Traditional Qualitative Risk Assessment	Semi-quantitative risk assessment	FAIR Risk Assessment
<b>Depth</b>	Assessment	Assessment	Analysis
<b>Focus</b>	Information Systems, Technology	IT, Compliance	Business services, processes, data
<b>Basis</b>	Subjective ratings	Subjective	Quantifiable information
<b>Orientation</b>	Controls	Controls	Business risk
<b>Output</b>	High/medium/low ratings	Semi-quantitative Likelihood x Impact=Risk (of what?)	Cost & time risk information
<b>Considers Event Timing &amp; Duration</b>	No	No	Yes



## COMMUNICATING RISK IN BUSINESS TERMS

Most organizations fail to communicate technical risk in terms that the business can use to make informed decisions, assess the current state against defined risk appetites, and confidently measure (or quantify) whether controls effectively reduce risk.

### Traditional (Current) Approach

Apply controls based on best practices and intuition with the hope that they will implicitly reduce our risk.

Risk reduction is expensive and hard to measure, as the approach is unfocused.



### Mature (Future) Approach

Assess likely threats and map them to our most critical assets. Design controls explicitly targeted toward these threat and asset combinations.

Risk reduction is focused on the areas of greatest risk and can be quantified.

# WHAT IS THE PROPOSED SOLUTION?

- ✓ Effective Management Requires Data and Models
- ✓ NISTIR 8286 Recommended Risk Quantification Methods
- ✓ Examples of where NISTIR 8286 + FAIR fits
- ✓ Enterprise - Annualized risks overview

## POLLING QUESTION #2

Do you have Cyber Risk Quantification (CRQ) capabilities in your organization?



Yes



No



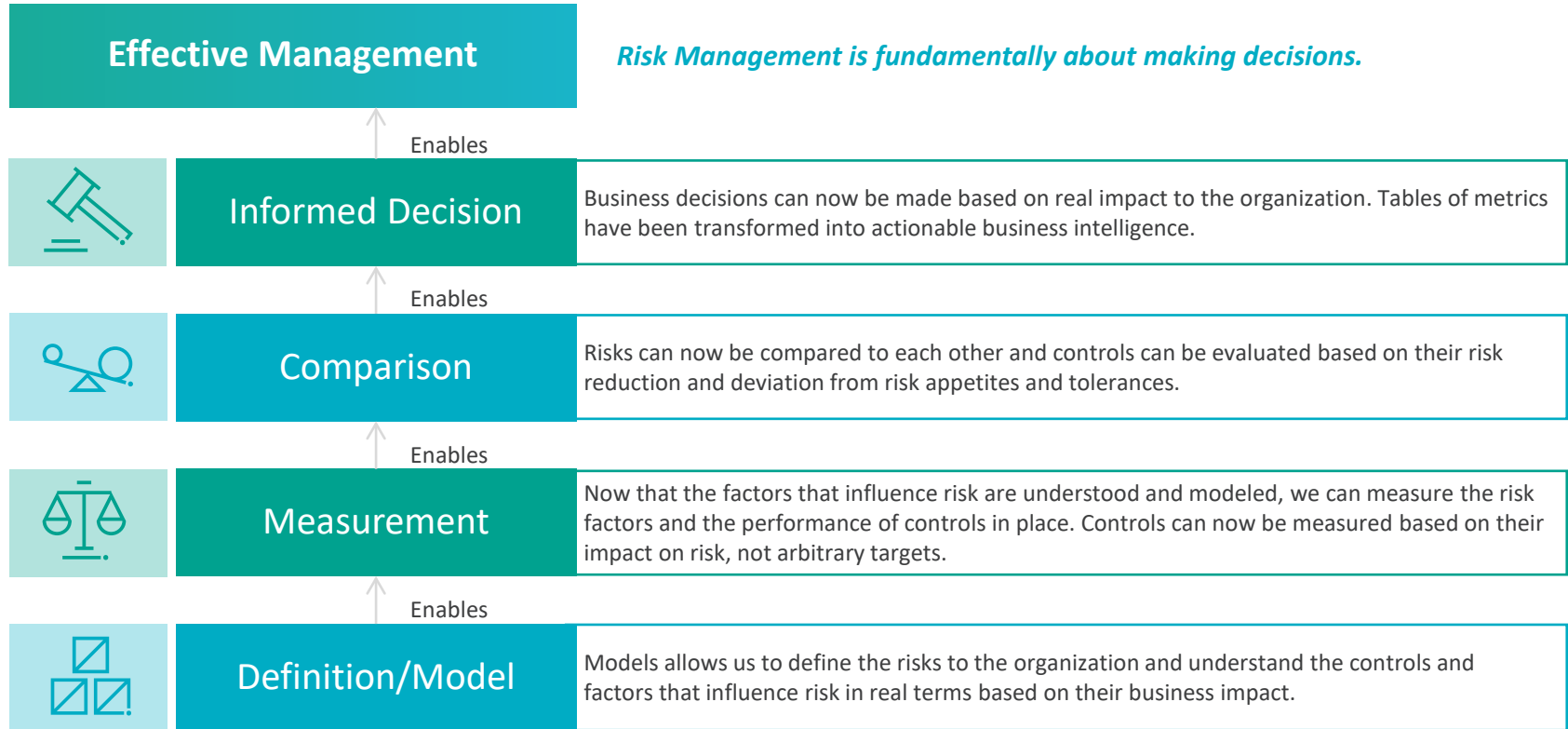
Not Sure



I have never heard of CRQ



# EFFECTIVE MANAGEMENT REQUIRES DATA AND MODELS



# NISTIR 8286 RECOMMENDS QUANTIFYING CYBER RISK

There are proven methods available for performing CSRM and integrating the results.

## Quantifying Risk in Financial Terms

Improving the measurement methods used in CSRM, through the use of cybersecurity risk registers, can improve the quality of the risk information provided to ERM.

## Communicating Risk

Improved communications will also help executives and corporate officers understand the challenges that cybersecurity professionals face when providing those professionals with the information they are accustomed to receiving for other types of risk.

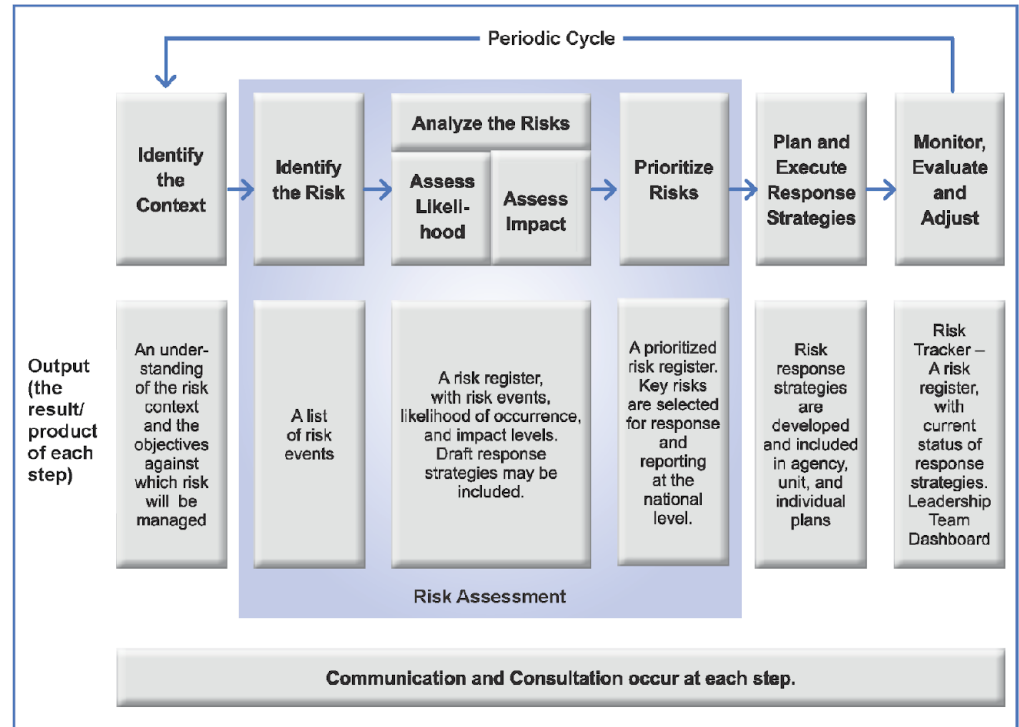


Figure 2: Notional Risk Management Life Cycle

# NISTIR 8286 RECOMMENDED RISK QUANTIFICATION METHODS

Examples of techniques for estimating the probability that a risk event will occur include:

## Bayesian Analysis

A model that helps inform a statistical understanding of probability as more evidence or information becomes available.

**Example:**

## Monte-Carlo

A simulation model that draws upon random sample values from a given set of inputs, performs calculations to determine results, and iteratively repeats the process to build up a distribution of the results.

**Example:** FAIR

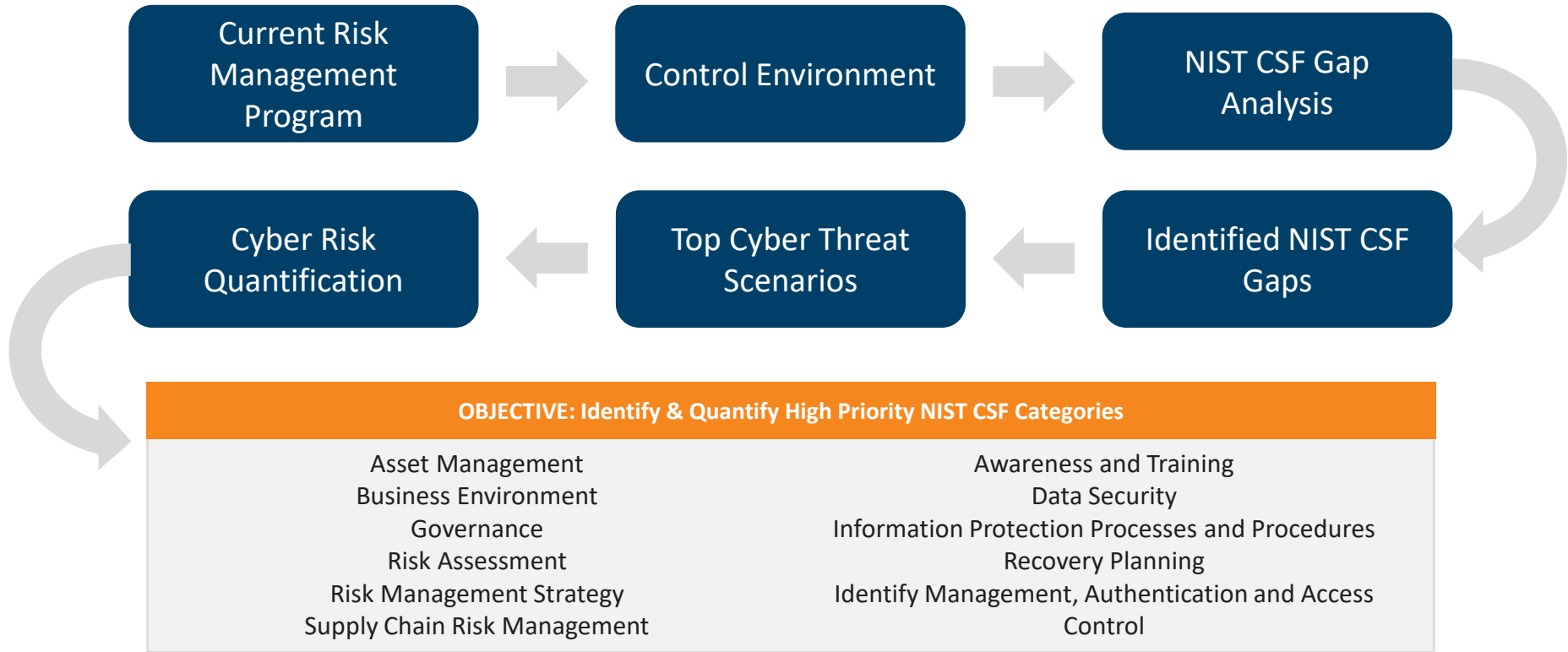
## Event Tree Analysis

A modeling technique that represents a set of potential events that could arise following an initiating event from which quantifiable probabilities could be considered graphically.

**Example:** ISO31000

Methodologies to Quantify Risk

# CYBER RISK QUANTIFICATION INFORMS DECISION MAKING – NIST -> CRQ ROADMAP





# EXAMPLES OF WHERE NISTIR 8286 + FAIR FITS

The FAIR Enterprise Model is complementary to many other industry and leading practice cybersecurity risk frameworks. The FEM is a tool that enables existing risk management concepts.

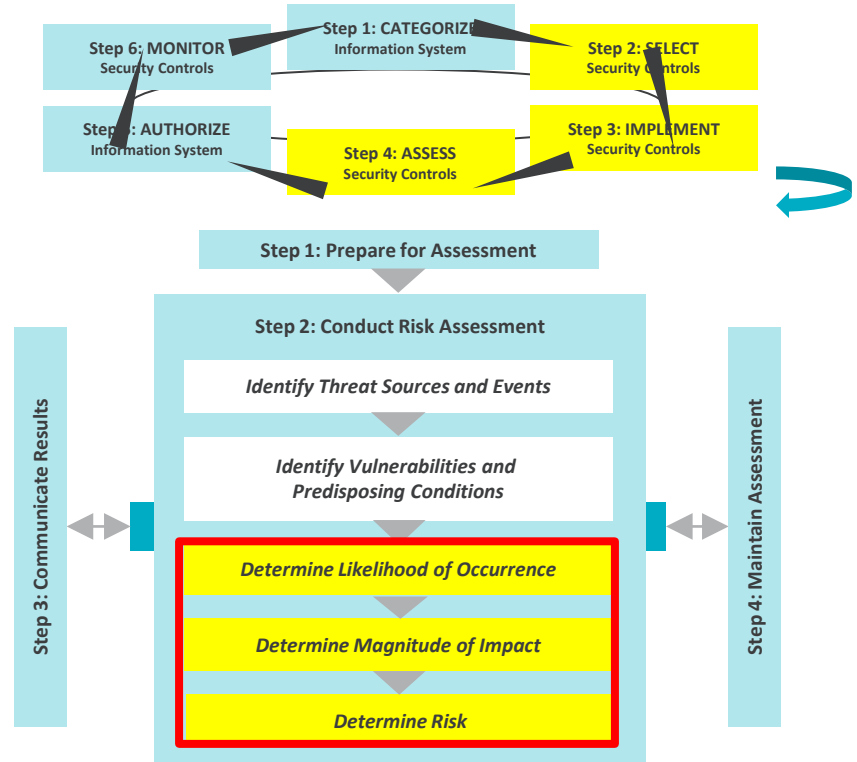
- **NIST Risk Management Framework (RMF)** – The FEM can be used to support operational decision making in the Select, Implement, and Assess security controls steps of the NIST RMF.
- **Top Risk Identification & Assessment** – The FEM can complement a traditional NIST 800-30 risk assessment by quantifying likelihood, magnitude, and impact of risks identified.



NIST SP 800-30 defines quantitative risk assessment as 1 of 3 approaches, in addition to qualitative and semi-qualitative.

The FEM enables organizations to incorporate quantitative analysis where historically cost or skill level was prohibitive.

- **NIST Cybersecurity Framework (CSF)** – Quantitative risk assessment enables advancements in Implementation Tier maturity (i.e. moving from Repeatable to Adaptive) at several levels of the NIST CSF. NIST has established FAIR as an Informative Reference to the NIST CSF.
- **NISTIR 8286** – A recent (published Oct 2020) NIST publication cites FAIR risk analysis as an established quantitative risk analysis methodology.



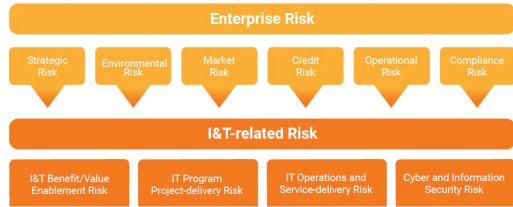
NIST RMF / NIST SP 800-30

# FAIR CRQ - COMPLEMENTARY TO RISK MGMT. FRAMEWORKS – RECOMMENDED

COSO Cube (ERM)



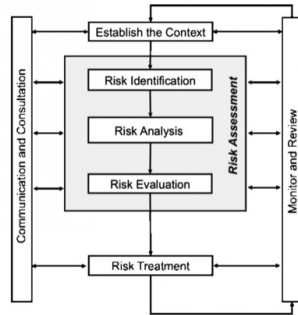
ISACA IT Risk Framework v2.0



Most risk mgmt. frameworks **do not prescribe a specific approach** to identifying, analyzing and prioritizing risk and leave it to the risk practitioners to select their preferred analytics model. NISTIR8286 now recommends FAIR as complementary, so do COSO & ISACA RMF 2.0.

This is where **FAIR** comes in and can be used to:

ISO31000 Risk Mgmt. Process



NIST Cybersecurity Framework



- **Identify top risks**, according to the FAIR risk scenario definitions
- **Quantify risk**, in monetary terms
- **Evaluate the efficacy of treatment options**, in terms of possible risk reduction
- **Communicate risk in a language than everyone understands**, including at board level

# EXPECTED OUTCOMES – QUANTITATIVE RISK MANAGEMENT PROGRAM WITH FAIR

Proposed outcomes from the FAIR Enterprise Model:

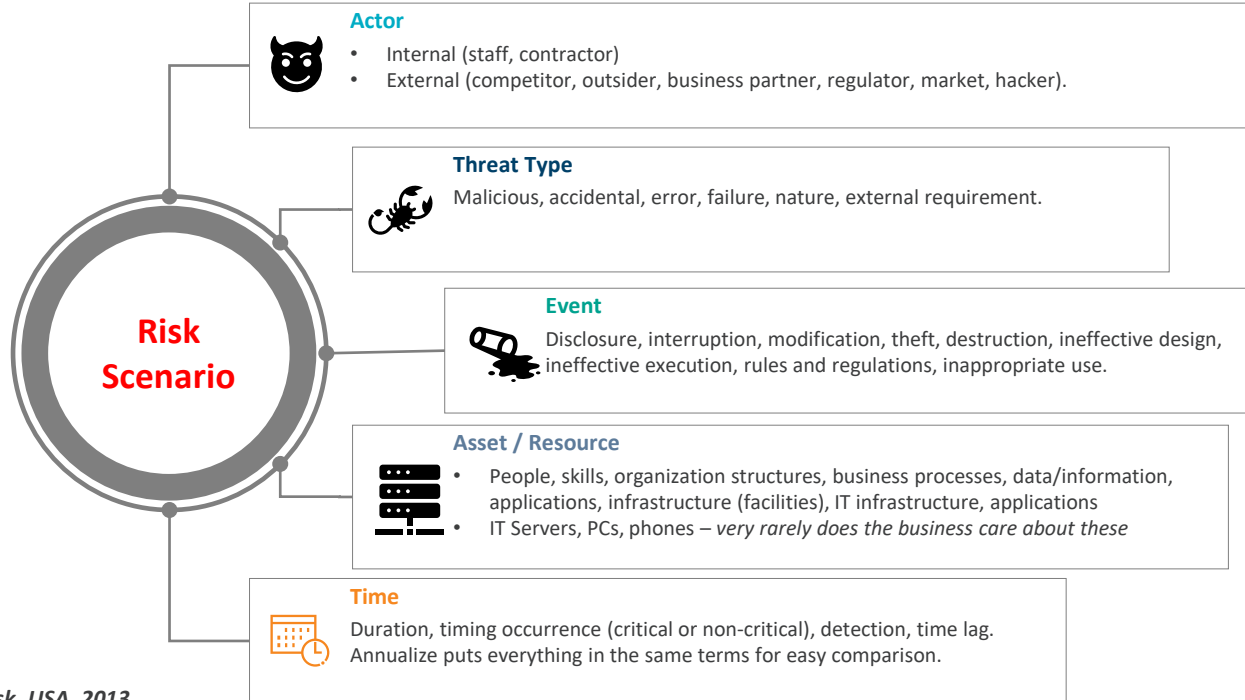
- **Establish Risk Register** to establish a common language around IT risks, creating consistent visibility on the management of those risks.
- **Top Risk Identification & Assessment** to establish a continuous process to regularly identify, quantify, and analyze organizational risks and business impact.
- **Comparative Analysis** to effectively triage risk scenarios based on level of criticality to appropriately identify high priority risk items.
- **Risk Appetite Definition** to establish risk tolerance levels in order to prescribe optimized risk treatment options.

Executing these outcomes requires a phased approach that builds on previous activities.



# RISK SCENARIO STRUCTURE

Risk scenario scoping at the is a foundational first step towards risk quantification. Framing up risk scenarios in this manner is a great first step in the right direction.



Source: ISACA, COBIT 5 for Risk, USA, 2013

# ENTERPRISE - ANNUALIZED RISKS OVERVIEW

The top risks, as identified by their average loss exposure, are plotted below. Additionally, 90<sup>th</sup> percentile and maximum (1/50,000 odds) values are listed as catastrophic worst-case scenarios.



## What are our top annualized risks?

Scenario	Scenario Description	Asset	Loss Effect	Average	90th %	Maximum
S6: HCI Theft	What is the risk associated with <b>internal users</b> causing a loss of <b>confidentiality</b> of <b>*COMPANY* Trade Secrets</b> via <b>theft of data</b> ?	*COMPANY* HCI / Trade Secrets	Confidentiality	\$20.4M	\$18.7M	\$612.4M
S2: HCI Malware	What is the risk associated with <b>cyber criminals</b> causing a loss of <b>confidentiality</b> of <b>*COMPANY* Trade Secrets</b> via a <b>targeted malware</b> ?	*COMPANY* HCI / Trade Secrets	Confidentiality	\$19.6M	\$747K	\$913.4M
S5: B2C PII Phishing	What is risk associated with a <b>hacktivist</b> causing a loss of <b>confidentiality</b> of <b>customer PII</b> by gaining access to <b>*COMPANY*</b> systems via <b>phishing</b> ?	B2C Customer PII	Confidentiality	\$14.3M	\$29.4M	\$257.8M
S8: HCI on Unsanctioned Cloud	What is the risk associated with <b>privileged insiders</b> causing a loss of <b>confidentiality</b> of by means of placing <b>*COMPANY* HCI / Trade Secrets</b> on <b>unsecured, unsanctioned cloud systems</b> ?	*COMPANY* HCI / Trade Secrets	Confidentiality	\$12.4M	\$14K	\$914.4M
S2: CHD Malware Attack	What is the risk associated with a <b>cyber criminal</b> causing a loss of <b>confidentiality</b> of <b>cardholder data</b> by gaining access to the <b>*COMPANY*</b> network and executing a <b>targeted malware attack</b> ?	B2C Cardholder Data	Confidentiality	\$9.5M	\$19M	\$53.3M

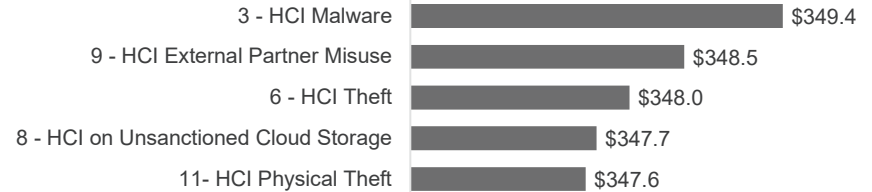
# ENTERPRISE - 90<sup>TH</sup> PERCENTILE AND RISK APPETITE OVERVIEWS



## What Single Event Would Cost The Most?

Sorting scenarios by single event loss magnitude allows us to view the scale of an event's loss, assuming it were to happen.

### Top Scenarios By 90<sup>th</sup> Percentile Per Event Loss Magnitude (in millions)

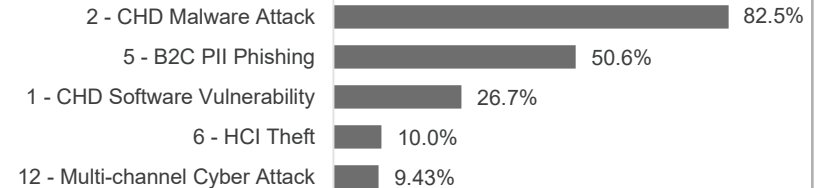


## Which scenarios are likely to cost more than \$3M next year?

Scenarios can also be sorted by the probability that they will exceed a given risk appetite.

In this view, scenarios are ranked by the probability that they will exceed a \$3M threshold in a given year.

### Probability of Exceeding \$3M



# TOP RISKS QUANTIFICATION – ENTERPRISE RISK REGISTER

Asset	Threat External Actor						Privileged Insider (incl. External Partner)			Non-privileged Insider
	Method Device Theft	Vulnerability Exploit	DDOS	Phishing / Social Eng.	Malware / Network Intrusion	Credential Theft	Misconfiguration	Data Exfiltration	Accidental Disclosure	Credential Theft
B2C PII In Digital Assets	M <sup>C</sup>	\$67.2M <sup>C</sup>	N/A	\$14.3M <sup>C</sup>	\$2M <sup>C</sup>	\$16.3M <sup>C</sup>	M <sup>C, A</sup>	M <sup>C</sup>	L <sup>C</sup>	L <sup>C</sup>
E-Commerce Capability	N/A	L <sup>A</sup>	\$57K <sup>A</sup>	M <sup>A</sup>	N/A	L <sup>A</sup>	L <sup>A</sup>	N/A	N/A	L <sup>A</sup>
Order Fulfillment	N/A	H <sup>A</sup>	L <sup>A</sup>	M <sup>A</sup>	N/A	H <sup>A</sup>	#4 <sup>A</sup>	N/A	N/A	L <sup>A</sup>
B2C Cardholder Data	\$553K <sup>C</sup>	\$3M <sup>C</sup>	N/A	TBD	\$11.3M <sup>C</sup>	TBD	TBD	TBD	TBD	L <sup>C</sup>
*COMPANY* HCI / Trade Secrets	\$5.9M <sup>C</sup>	H <sup>C</sup>	N/A	M <sup>C</sup>	\$18.9M <sup>C</sup>	H <sup>C</sup>	\$12.2M <sup>C</sup>	\$28.6M <sup>C</sup>	L <sup>C</sup>	L <sup>C</sup>
Partner Confidential Data	M <sup>C</sup>	H <sup>C</sup>	N/A	M <sup>C</sup>	TBD	H <sup>C</sup>	M <sup>C, A</sup>	\$2.8M <sup>C</sup>	L <sup>C</sup>	L <sup>C</sup>

## Legend

- C – Loss of Confidentiality
- A – Loss of Availability
- I – Loss of Integrity

- Average ALE of greater than or equal to \$20M
- Average ALE of greater than or equal to \$3M and less than \$20M\*
- Average ALE of greater than or equal to \$1M and less than \$3M
- Average ALE of less than \$1M

- Not Yet Quantified, Qualitative High
- Not Yet Quantified, Qualitative Medium
- Not Yet Quantified, Qualitative Low
- N/A – Risk does not apply to selection

\* - Materiality for financial reporting is approximately \$5M, as such risks with an average ALE of \$5M are considered at least Moderate

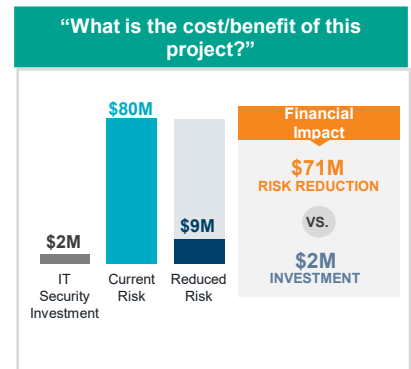
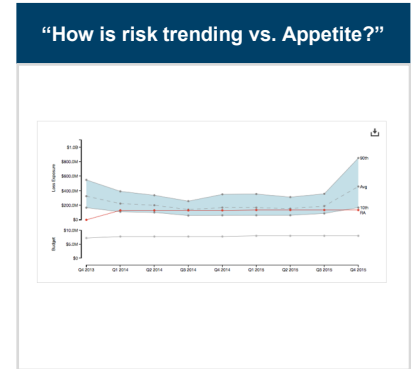


# ANSWERING BUSINESS QUESTIONS WITH CYBER RISK QUANTIFICATION

Protiviti has best-in-class FAIR Risk Quantification insights and credentials. We have set out below and on the following page some examples of our tools and the accelerators that we will use during our engagement with you.



Protiviti is a Founding Advisory Partner for the FAIR Institute. We see examples of typical applications of cyber risk quantification and the types of questions and scenarios CRQ can address.





## Next Steps

## POLLING QUESTION #3

### Would you be interested in learning more about ERM or CRQ?



Yes, I would love to have a free 30-min consultation about ERM &/or CRQ



Yes, please send me thought leadership regarding CRQ



Yes, please send me thought leadership regarding ERM



Nah, I am good



# ADDITIONAL RESOURCES AVAILABLE

Protiviti Developed Materials – for the latest insights visit:

[www.protiviti.com/FAIR](http://www.protiviti.com/FAIR)

[www.protiviti.com/ERM](http://www.protiviti.com/ERM)

## CRQ Smart Sheet

MAKE BETTER DECISIONS WITH MEANINGFUL CYBER PROGRAM INTELLIGENCE.

Answer the Board's questions and Quantitative Cyber Risk Measurements.

Do we have enough cyber insurance?  
Are we doing enough to minimize risk? How much would a breach cost?  
Are we spending on cybersecurity budget on the right things? What is the ROI?  
How much risk do we have? Are we spending too much on too little?

**Quantitative Risk Assessment**      **Qualitative Risk Assessment**

1. Risk is a complex and multifaceted issue. How can you get a clear picture of the risk landscape?  
2. Risk is not quantifiable in a single number. How can you get a clear picture of the risk landscape?  
3. Risk is not quantifiable in a single number. How can you get a clear picture of the risk landscape?  
4. Risk is not quantifiable in a single number. How can you get a clear picture of the risk landscape?

1. Risk is a complex and multifaceted issue. How can you get a clear picture of the risk landscape?  
2. Risk is not quantifiable in a single number. How can you get a clear picture of the risk landscape?  
3. Risk is not quantifiable in a single number. How can you get a clear picture of the risk landscape?  
4. Risk is not quantifiable in a single number. How can you get a clear picture of the risk landscape?

protiviti

## Protiviti Subject Matter Experts:

- **Rebecca Nilson** – [Rebecca.Nilsson@protiviti.com](mailto:Rebecca.Nilsson@protiviti.com)
- **George Quinlan** – [George.Quinlan@protiviti.com](mailto:George.Quinlan@protiviti.com)



*Face the Future with Confidence*

**Thank you!**