

**RSA** Conference 2018

San Francisco | April 16 – 20 | Moscone Center



#RSAC

SESSION ID: STR-W02

# IMPLEMENTING A QUANTITATIVE CYBER RISK FRAMEWORK: A FINSRV CASE STUDY

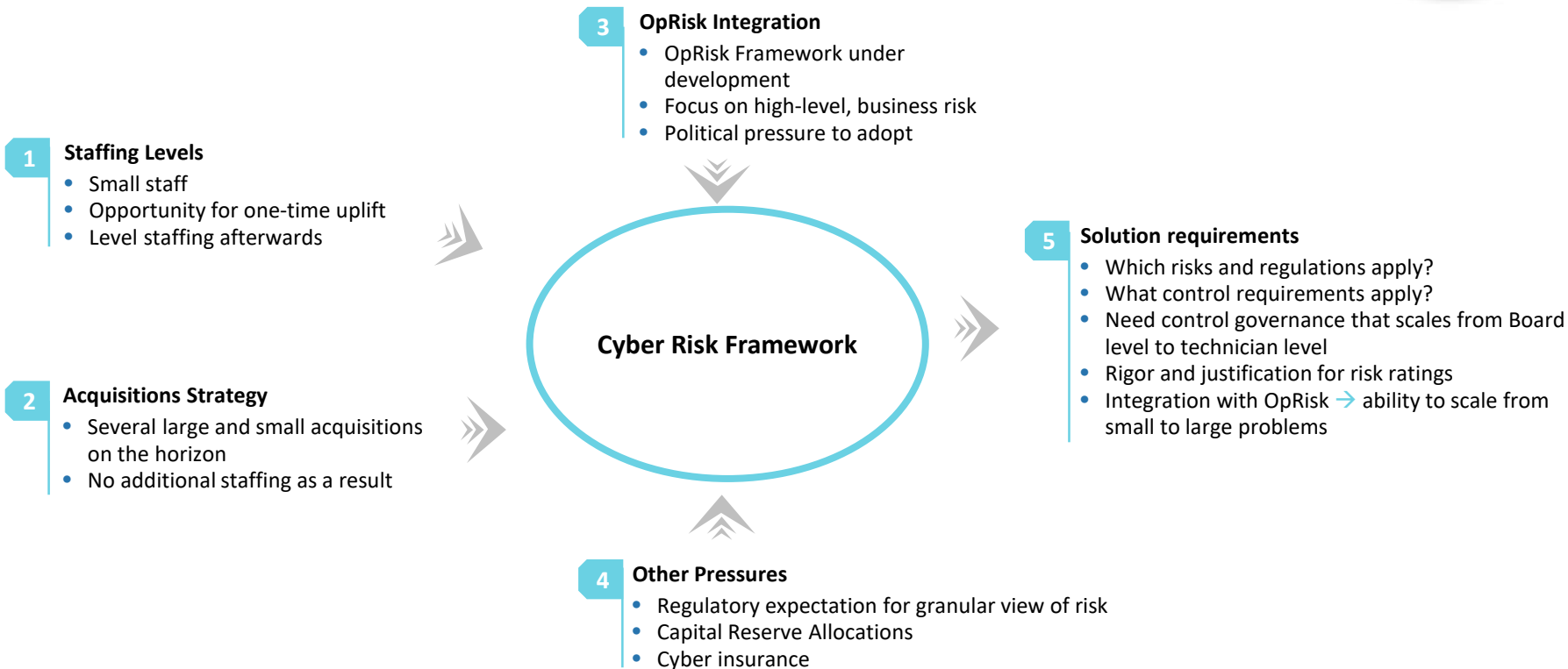
**Jack Freund, Ph.D.**

Director, Cyber Risk

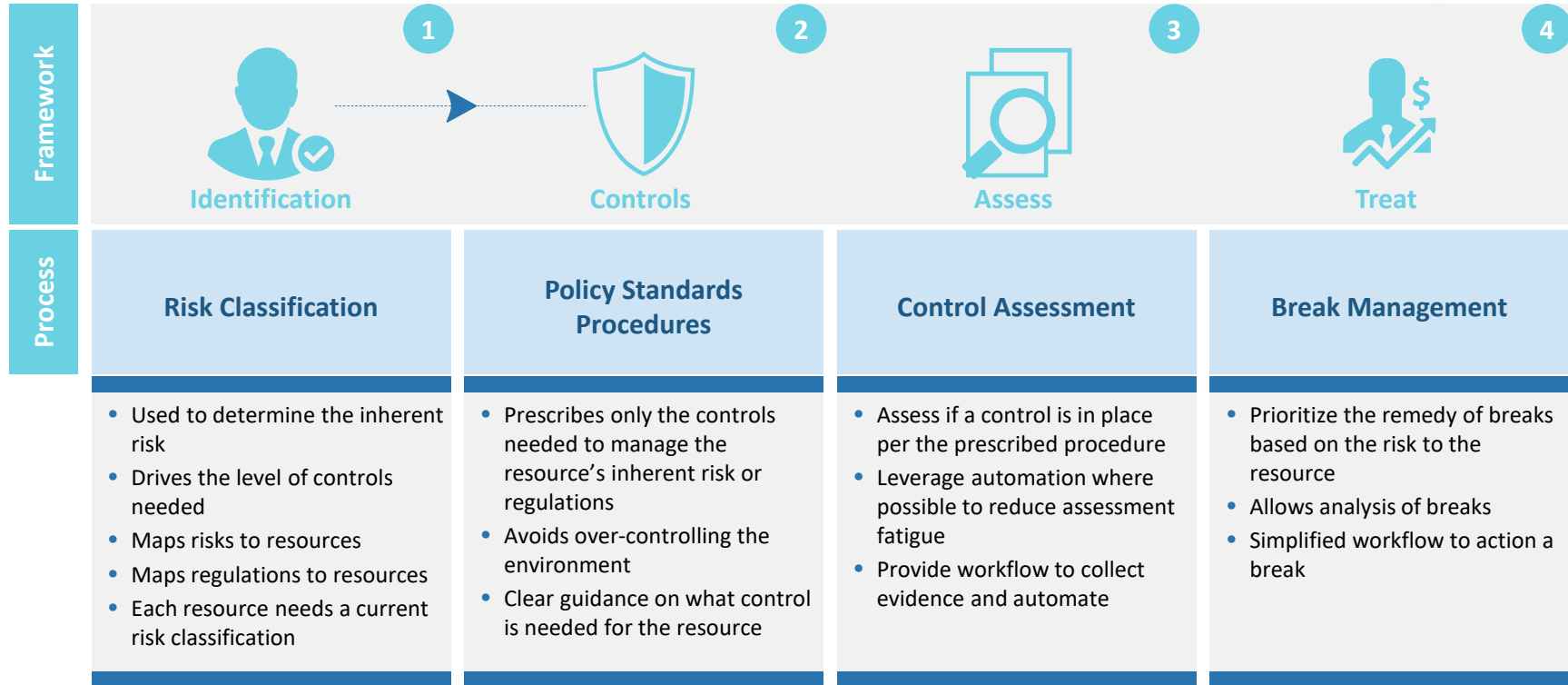
TIAA

@jackfreund3

# Impetus for Cyber Risk Framework



# Overview of Cyber Risk Framework



# Control Framework Overview



The Information Technology Policy and Control Framework allows articulation of requirements for technical configurations, processes, and behaviors throughout the IT organization.

	Definition	Example	
<b>1</b>  <b>Policy</b>	<ul style="list-style-type: none"><li>A collection of standard statements indicating Purpose, Scope, Objectives and Control (or Compliance) requirements that is not relative to a specific technology but is ubiquitous throughout all of IT and organized by high level directives.</li></ul>	<ul style="list-style-type: none"><li>IT Policy</li></ul>	<b>What</b> General/ Descriptive  Specific/ Prescriptive <b>How</b>
<b>2</b>  <b>Standard</b>	<ul style="list-style-type: none"><li>A standard is a statement designed to meet the security expectations and requirements of our regulators, auditors, and institutions. They are not statements of capability but expectations on our organization to which we must adhere.</li></ul>	<ul style="list-style-type: none"><li>Users must not be able to construct passwords that are identical to those used the last twelve (12) times they have changed their password.</li></ul>	
<b>3</b>  <b>Procedure</b>	<ul style="list-style-type: none"><li>An instruction or set of instructions which inform staff of how IT standards are to be implemented. Procedures also detail the testing criteria used to measure a passing outcome or a break during an assessment. A procedure can define a technical configuration setting or define requirements for a process.</li></ul>	<ul style="list-style-type: none"><li>Windows 2008 R2 and 2012 R2 Member Servers will be set to record the previous 12 passwords.</li></ul>	

# Authoritative Sources



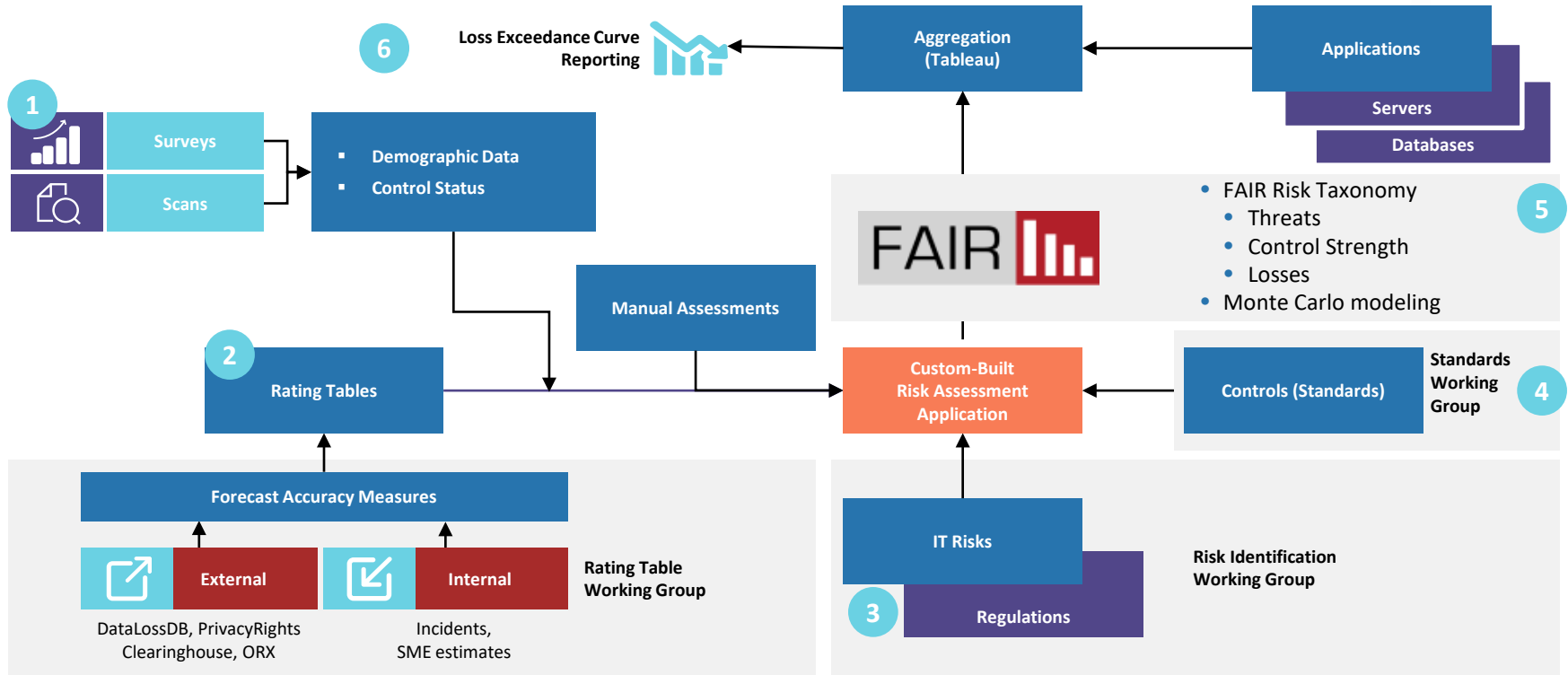
Authoritative Sources map regulatory guidance to IT standards, which aids in the identification of gaps. Authoritative Sources should be regularly reviewed for completeness and appropriateness.

1	Regulators	Auditors	Customers
		<b>Institutions</b>	<b>Individuals</b>
2	<b>Authoritative Sources</b>		
	<ul style="list-style-type: none"> <li>• FFIEC</li> <li>• Sarbanes-Oxley</li> <li>• NIST Cyber Security</li> <li>• State Privacy Laws</li> </ul>	<ul style="list-style-type: none"> <li>• SSAE16 Type 2</li> <li>• COBIT</li> <li>• NIST</li> <li>• ISO</li> </ul>	<ul style="list-style-type: none"> <li>• 23 NYDFS 500</li> <li>• FACT ACT – Red Flag</li> <li>• SEC OCIE</li> <li>• National Futures Association</li> </ul>
3	<b>Standards Groupings/Control Programs</b>		
	<ul style="list-style-type: none"> <li>• Cybersecurity Management</li> <li>• Cyber Risk Management</li> <li>• IT Personnel Security</li> <li>• IT Physical Security</li> <li>• IT Operations Management</li> </ul>	<ul style="list-style-type: none"> <li>• IT Security Monitoring &amp; Response</li> <li>• IT Communications Management</li> <li>• Workforce Access Control</li> <li>• IT Network Security</li> <li>• Supplier Management</li> </ul>	<ul style="list-style-type: none"> <li>• IT Application Mgmt.</li> <li>• IT Business Continuity</li> <li>• IT Compliance and Privacy</li> <li>• IT Event and Incident Management</li> <li>• Customer Authentication</li> </ul>



Authoritative Sources are mapped to IT standards to ensure they meet the expectations of regulators, auditors, and customers.

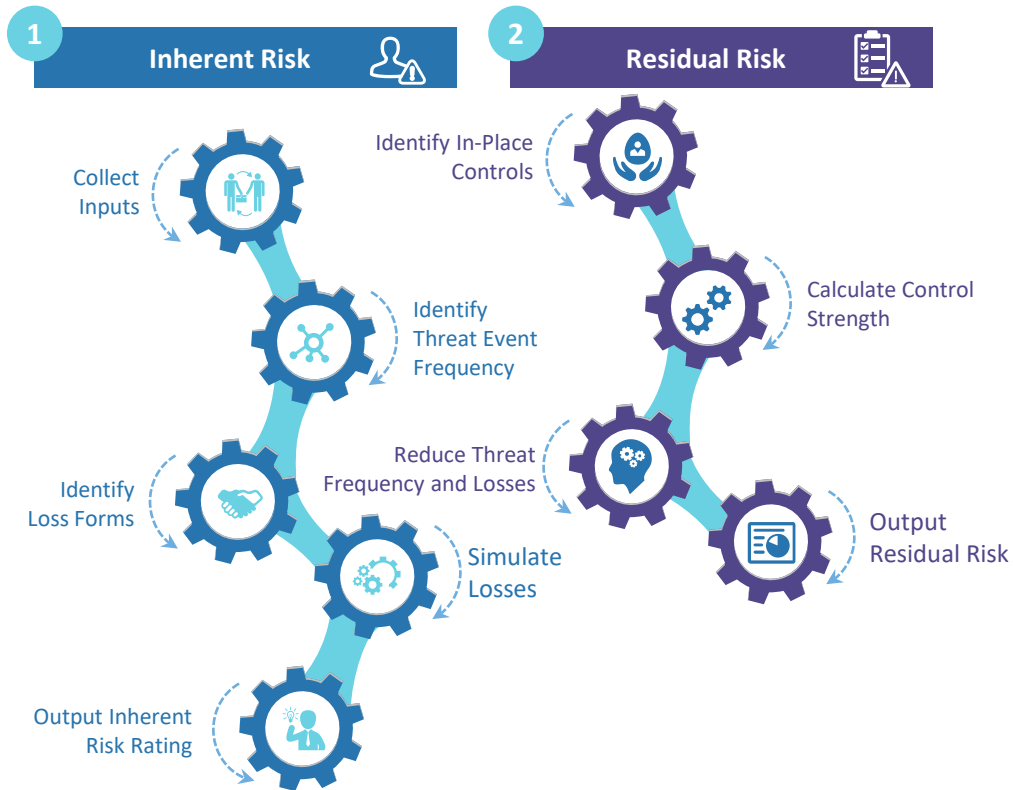
# IT Risk Central Overview



# Risk Assessment Process, Scope, & Metrics



#RSAC

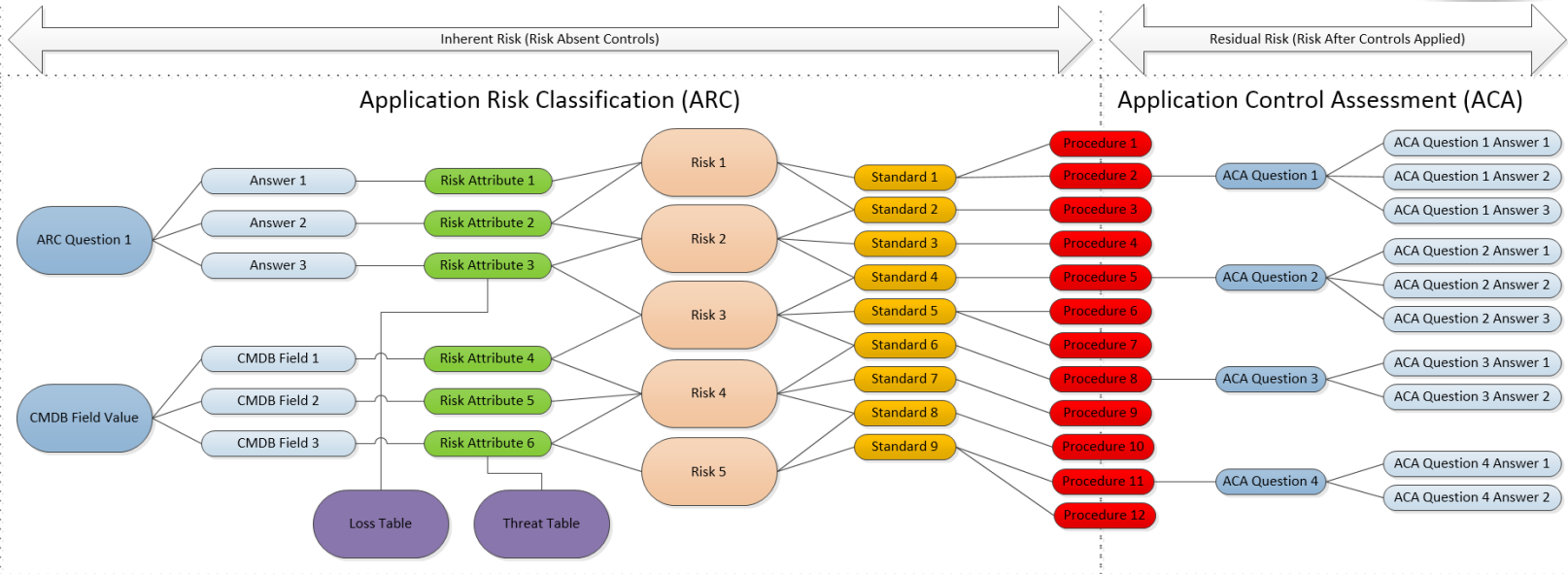


	3 Ex. Scope		4 Risk Visibility Metrics (KRIs)			5 Risk Operation Metrics (KPIs)	
	Assessment	Type	% Resources	% Controls	% in Appetite	% Completed Within SLA	Completed YTD
Business	Applications	I					
		R					
	IT Services Projects	I/R					
Infrastructure	Servers	I					
		R					
	Databases	I					
		R					
	Network	I					
		R					
	Workstations	I					
		R					
Third Party/ Data Centers	IOT	I/R					
		I/R					
	Cloud	I/R					
		I/R					
Third Party/ Data Centers	Facilities	I/R					
		I/R					
	Suppliers	I/R					
		I/R					
Subsidiaries	I/R						
	Data Transfers	I/R					

# Application Risk Assessment Details



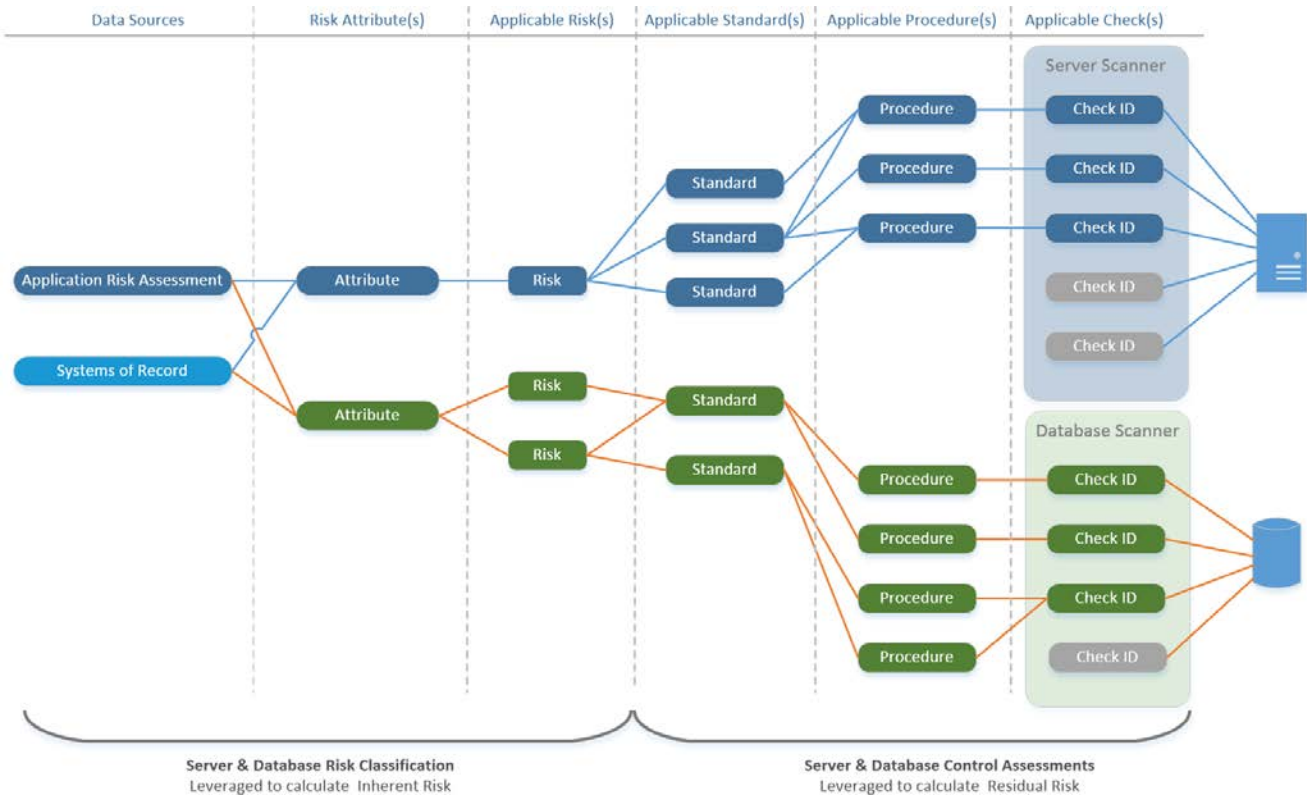
#RSAC



ARC Question	ARC Answers	Risk Attribute	Risk	Standard	Procedure	ACA Question	ACA Answers
How often in the course of a year is the application modified or changed?	<ul style="list-style-type: none"> <li>Once a year or less</li> <li>Once a quarter</li> <li>Every other month</li> <li>Once a month</li> <li>More than once a month</li> </ul>	<ul style="list-style-type: none"> <li>Resource Change Frequency : 1 or Less</li> <li>Resource Change Frequency : 4</li> <li>Resource Change Frequency : 6</li> <li>Resource Change Frequency : 12</li> <li>Resource Change Frequency : &gt; 12</li> </ul>	Erroneous change in an application or system by an authorized user	All internal development efforts must follow the Systems Development Life Cycle methodology and Change Management Processes.	All internal development efforts must follow the Systems Development Life Cycle methodology and Change Management Processes.	Is the Change Management process followed when changes are made to the application or other dependent components?	<ul style="list-style-type: none"> <li>Yes</li> <li>No</li> </ul>



# Infrastructure Risk Assessment Details



## Server & Database Risk Classification (SRC/DRC):

- Determine the applicability of IT Standards & Technical Procedures relevant to each server and database
- Informs inherent risk calculations

## Server & Database Control Assessment (SCA/DCA):

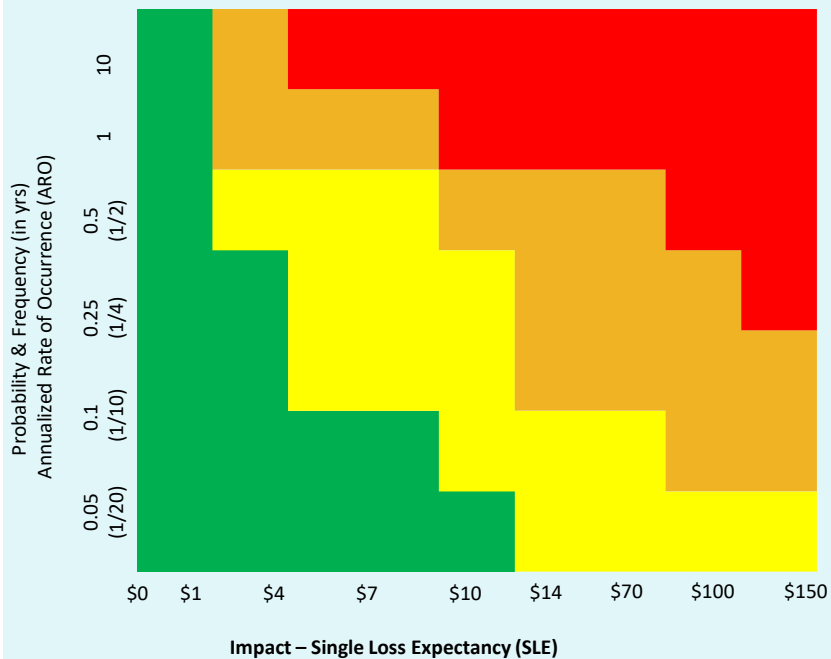
- Evaluate servers and databases against the relevant Technical Procedures
- Create breaks for deviations
- Informs residual risk calculations

# Risk Ratings – Translating Quant to Action



1

Example Cyber Risk Heatmap



2

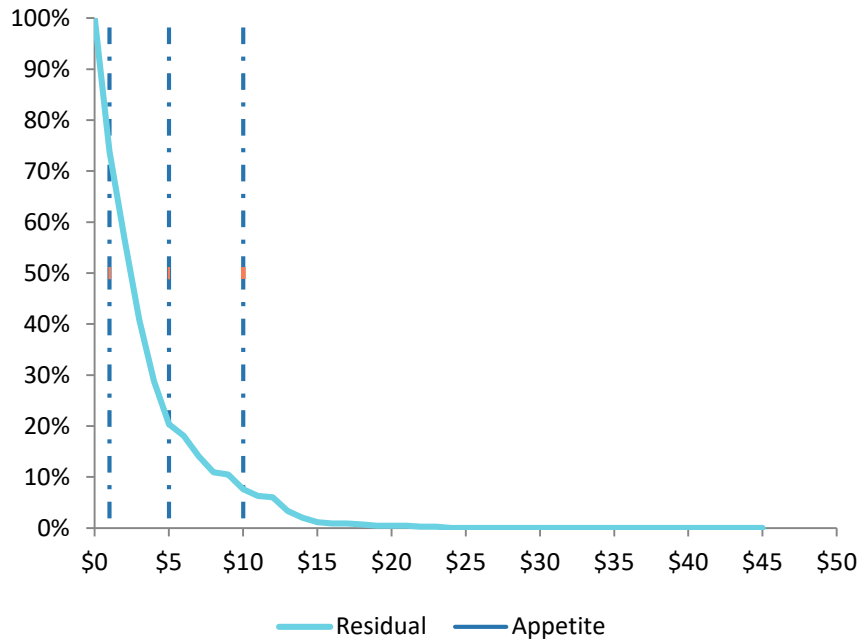
Ranking	ALE	Behavior
<b>Critical</b>	> \$14	All hands on deck, cost of resolution is a nonfactor, daily meetings (or more frequent) tracking to resolution
<b>High</b>	> \$8	Gains attention of upper management; plans are made to track concern to resolution in current or next period
<b>Moderate</b>	> \$1	Willingness of management to adjust plans and reallocate resources in the current or next few planning periods to remediate
<b>Low</b>	< \$1	Infrequent monitoring/review to ensure risk does not escalate

# Aggregate Risk Appetite Reporting using LECs



1

<Quarter> <LOB> LEC – Per Incident Loss Projections



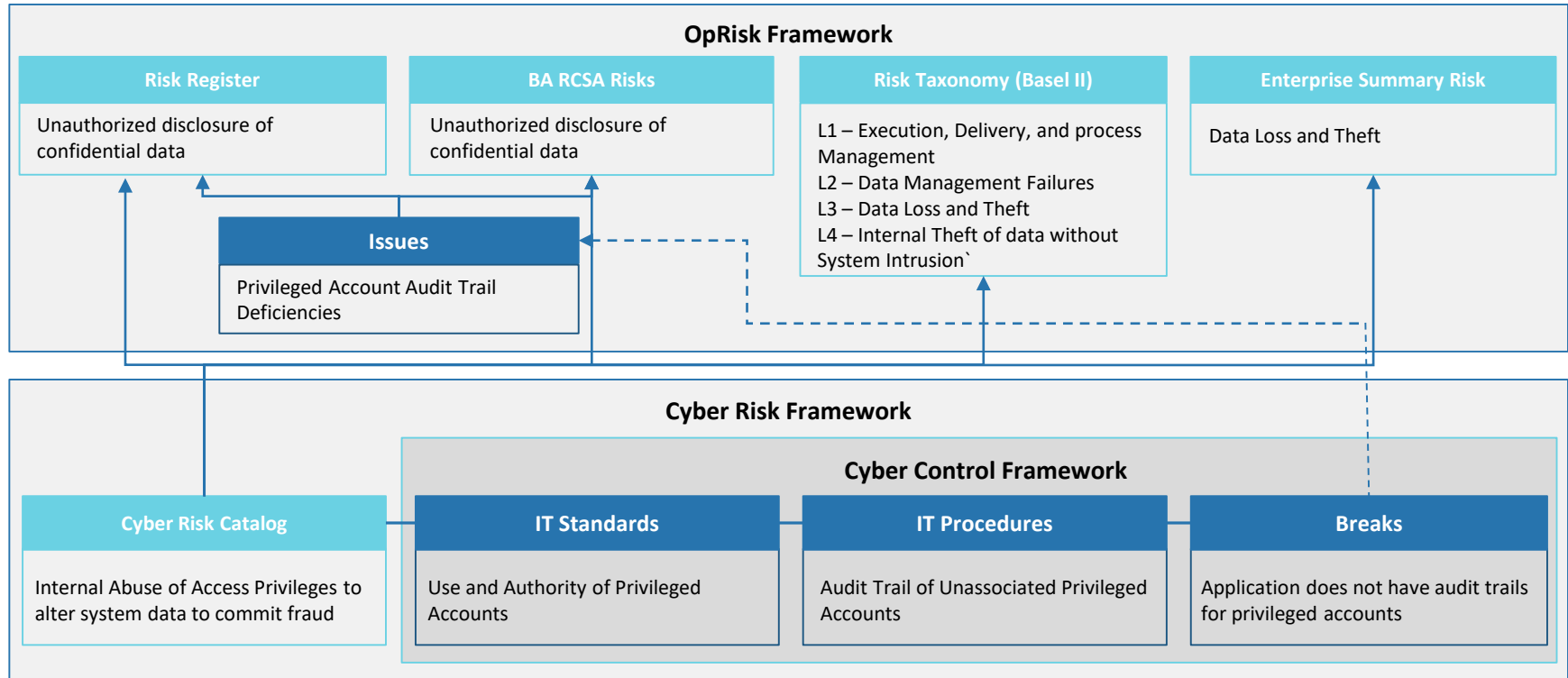
2

Appetite	Probability of Exceeding Appetite	# of Apps that Exceed Appetite
\$1	75%	25
\$5	18%	15
\$14	3%	8

You can use multiple appetite thresholds to begin socializing risk appetite

- 75% of <LOB> applications could contribute to a technology risk incident that exceeds the appetite due to having a residual risk (after considering in-place controls) higher than \$1
- Residual risk graph represents 500 critical/high inherent risk applications that completed the control assessment
- Reduction of residual risk can be accomplished through remediation of control gaps

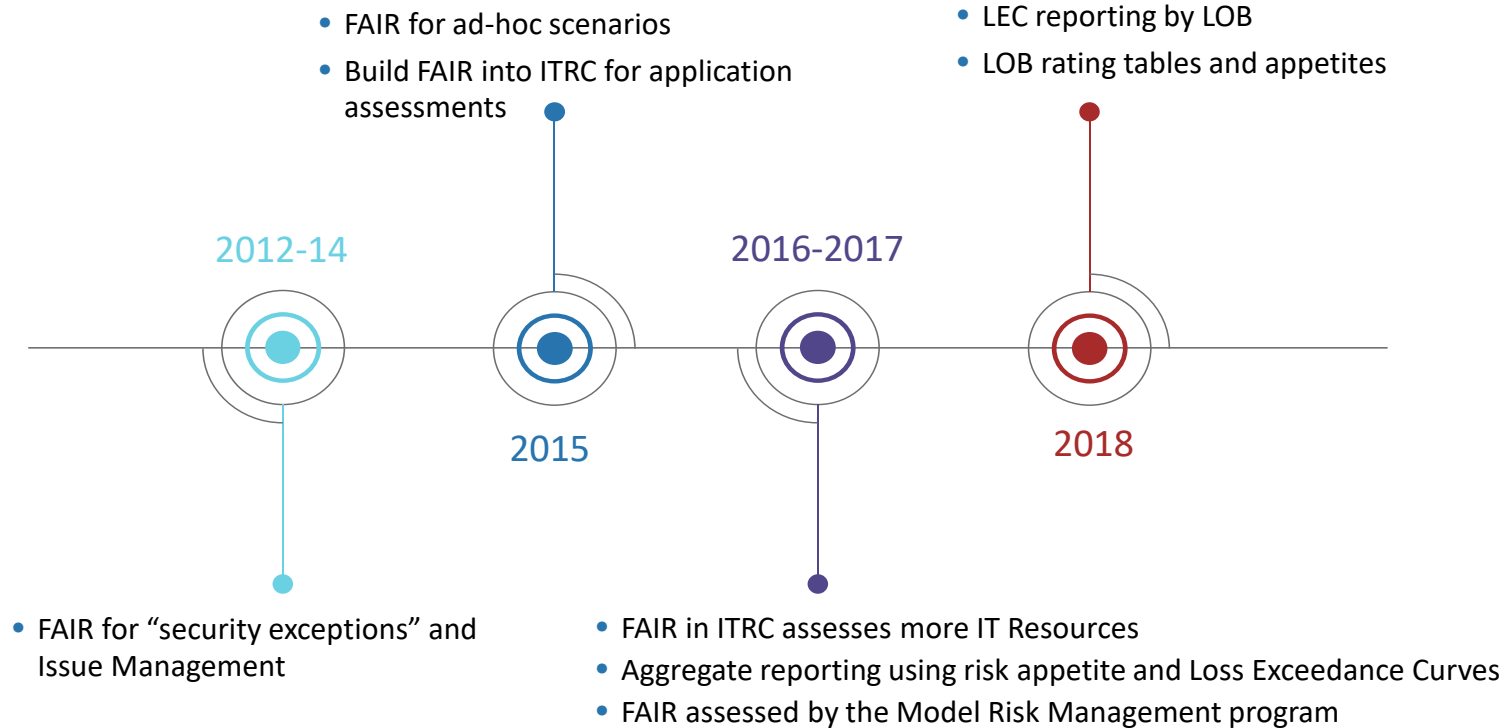
# OpRisk Integration



# History of Cyber Risk Quant



#RSAC



# Quant Cyber Risk Justification



## OpenGroup

- Independent IT Standards organization
- OpenFAIR Body of Knowledge (Since 2009)
  - Risk Ontology
  - Risk Analysis Process
- Individual Analyst Certification (Since 2013)
- FAIR/ISO Cookbook standard that outlines the process to integrate FAIR into any other security standard



## NIST Cybersecurity Framework (CSF)

- NIST recognized FAIR as a complementary standard to add economic dimensions to impact assessments (under industry resources)



## Federal Reserve, Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC)

- In the ANPR sent jointly by these three agencies, they are looking to for a consistent, repeatable, methodology to support measurement of cyber risk. FAIR was one of two methods identified
- Jay Restel from the Federal Reserve Bank of Cleveland identified publicly that FAIR will be an important component of cyber risk measurement for large banks



## Payment Cards Industry Data Security Standard (PCI-DSS)

- PCI's Risk Assessment Guideline in section 3 recommends compliance with NIST, ISO, and recommends FAIR as a risk framework to complement these two standards



## FAIR Book (2014)

- Published by TIAA employee and creator of FAIR
- Book was inducted into the Cyber Security Cannon in 2016 (Books all cyber security professionals should read)
- Referenced in 2016 book How to Measure Anything in Cybersecurity Risk (Douglas Hubbard) as a model that can be used to measure cyber risk. Douglas's books on risk measurement are required reading for the Society of Actuaries Enterprise Risk Management exams



## FAIR Institute (2013)

- Non-profit organization established in 2013 to promote the practice of cyber risk measurement and quantification
- FAIR is the primary methodology supported by the Institute

# Key Takeaways and Application



#RSAC

## Near term

Reevaluate Control Framework to articulate different levels of detail throughout the org

Assess and report on existing risk visibility and operations metrics. Red metrics are your friend. Be clear to stakeholders what you are and are not assessing.

Develop FAIR-compliant risk scenarios and tag them to existing assessment results (process or resource-level)

Identify automation opportunities and incorporate risk & reg statements, control requirements, and risk scenarios

Develop aggregate risk views to incorporate into ORM/ERM frameworks and initiatives.

## Long term