GRC Technology in Action

Viviana Campanaro – CISSP

December 8, 2020

© 2020 Jack Henry & Associates, Inc.®

Viviana Campanaro – CISSP
Security & Compliance Sales
ProfitStars

- 20 Years Cybersecurity & IT Compliance
- 10 Years in Financial Institutions
- ISSA, InfraGard, ISC2

Discussion Topics

- GRC
- Why GRC Platform
- GRC in Action
- Where to Start

It's a scary world…

"90% of financial institutions reported being targeted by malware"

"Cybercrime Up 600% Due To COVID-19 Pandemic"

"Ransomware attacks are estimated to cost $6 trillion annually by 2021"

"34% of businesses hit with malware took a week or more to regain access to their data."

"92% of malware is delivered by email"

"7 out of every 10 malware payloads were ransomware"

"Over 18 million websites are infected with malware at a given time each week."

"98% of cyber attacks rely on social engineering"

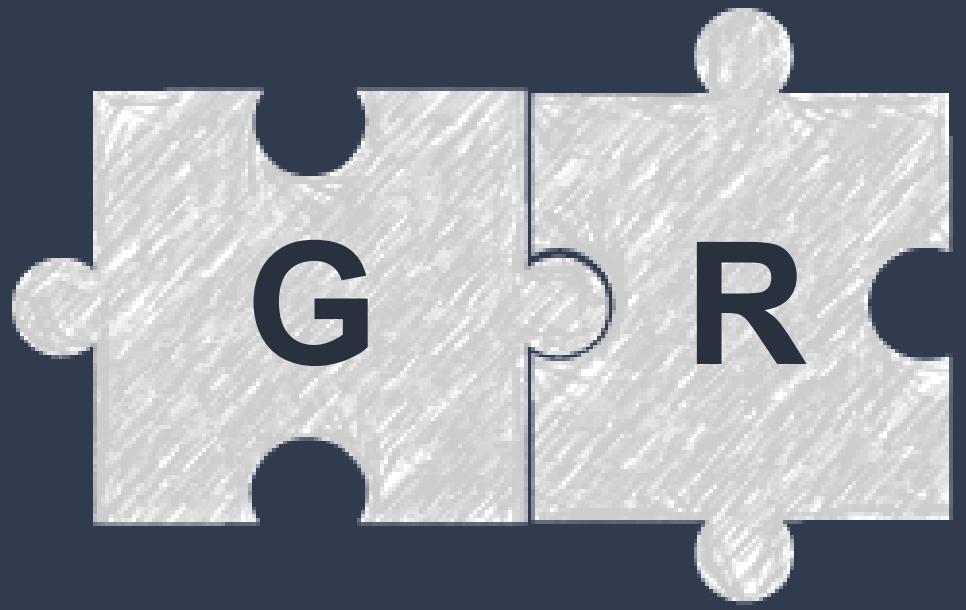
"The total malware infections have been on the rise for the last ten years"

© 2020 Jack Henry & Associates, Inc.®

Governance Risk & Compliance

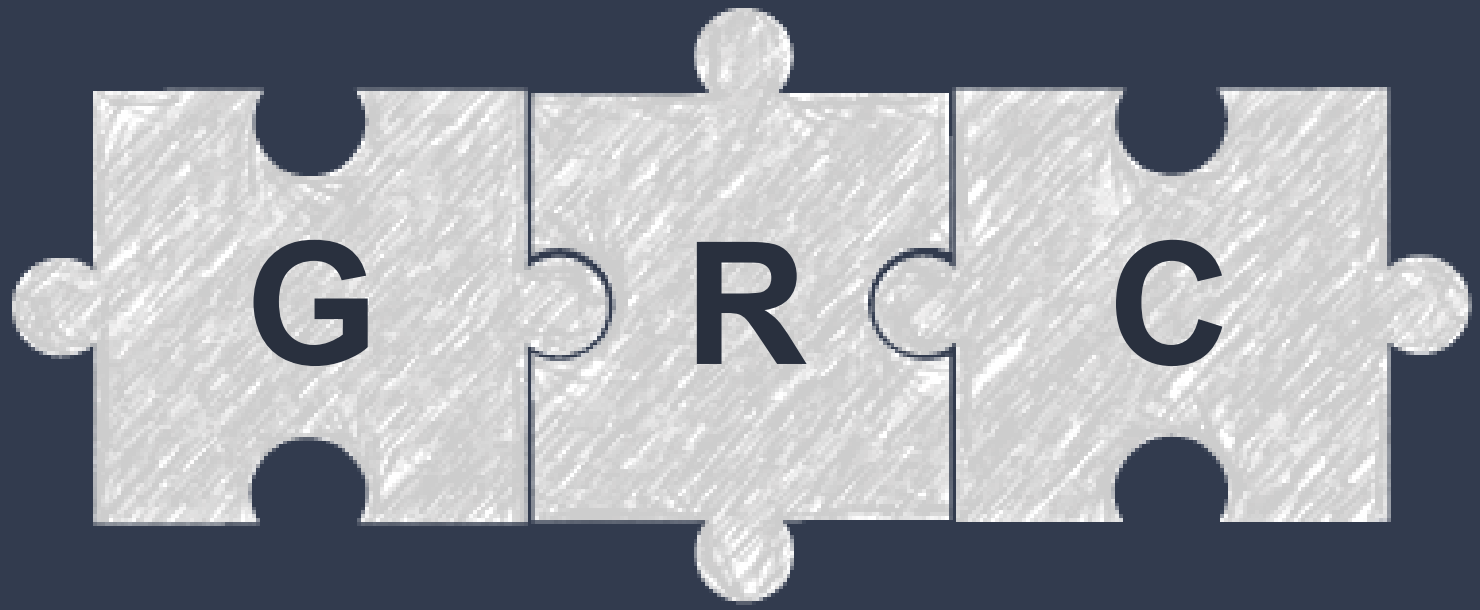
- ✓ Set business strategy & objectives
- ✓ Determine risk appetite
- ✓ Establish culture & values
- ✓ Develop internal policies
- ✓ Monitor/measure performance

Governance Risk & Compliance



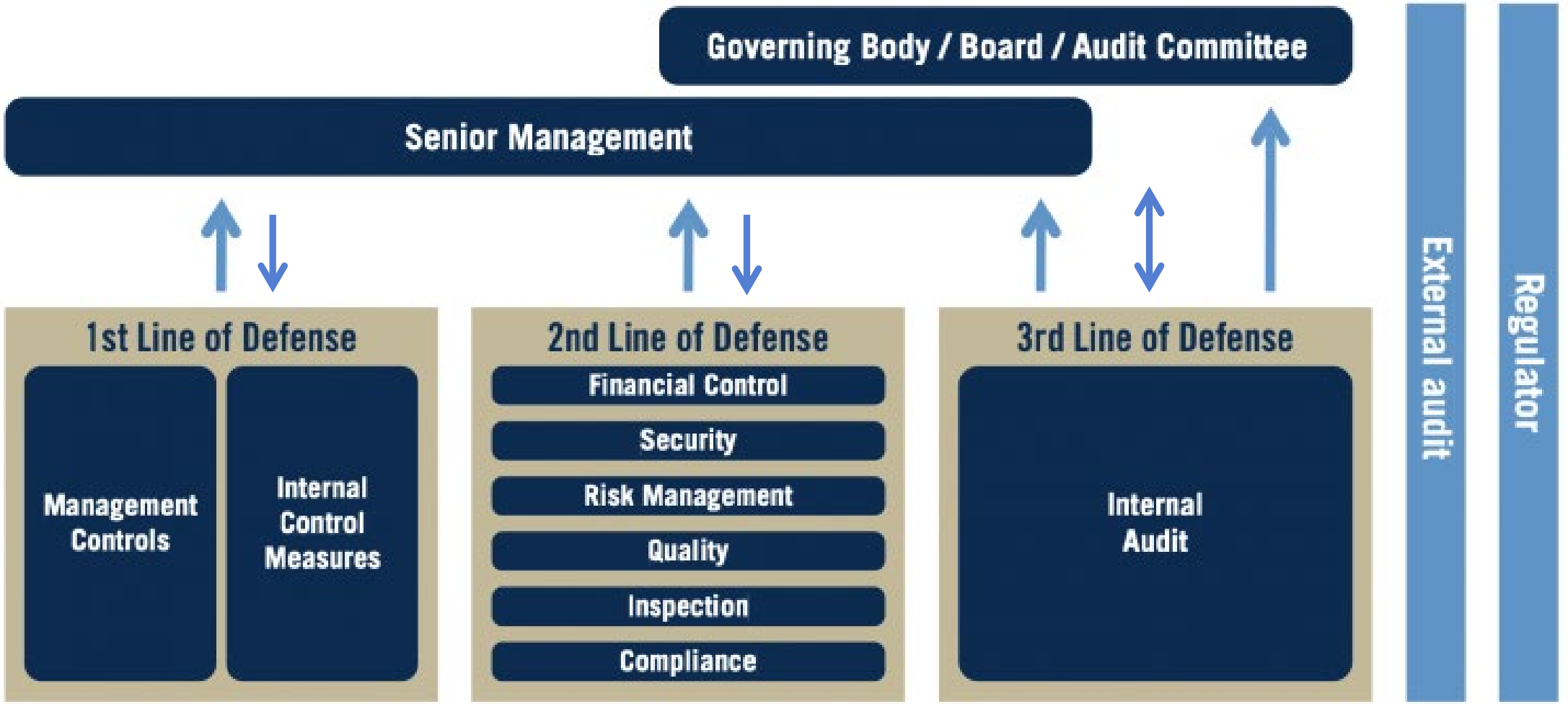
- ✓ Risk = Possibility of loss or damage created by an activity or person
- ✓ Seeks to Identify and Assess risks in order to Mitigate, Accept, Avoid or Transfer them

Governance Risk & Compliance



- ✓ Observance of relevant laws, regulations, and corporate policies
- ✓ Relies on governance standards and risk tolerance

The Three Lines of Defense Model



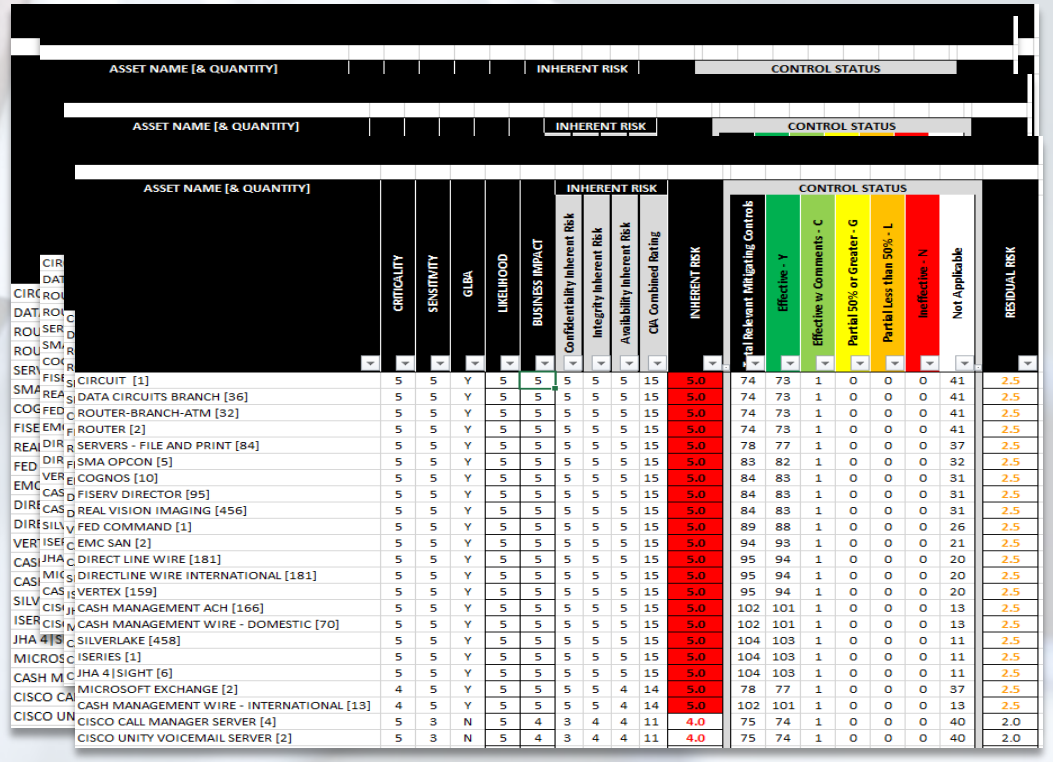
KEY: ↑ Accountability, reporting | ↓ Delegation, direction, resources, oversight | ↔ Alignment, communication coordination, collaboration

Source: IIA – Institute of Internal Auditors – www.na.theiia.org

© 2020 Jack Henry & Associates, Inc.®

Today's "Silo" Environment

- Business Continuity
- Risk Assessments
- Vendor Management
- Policies
- Security Training
- Audits/Exams
- Incident Response
- Reporting



ASSET NAME [& QUANTITY]	CRITICALITY	SENSITIVITY	GLBA	LIKELIHOOD	BUSINESS IMPACT	INHERENT RISK: Confidentiality Inherent Risk	INHERENT RISK: Integrity Inherent Risk	INHERENT RISK: Availability Inherent Risk	INHERENT RISK: CIA Combined Rating	INHERENT RISK	CONTROL STATUS: Partial Relevant Mitigating Controls	CONTROL STATUS: Effective - Y	CONTROL STATUS: Effective w Comments - C	CONTROL STATUS: Partial 50% or Greater - G	CONTROL STATUS: Partial Less than 50% - L	CONTROL STATUS: Ineffective - N	CONTROL STATUS: Not Applicable	RESIDUAL RISK
CIRCUIT [1]	5	5	Y	5	5	5	5	5	15	5.0	74	73	1	0	0	0	41	2.5
DATA CIRCUITS BRANCH [36]	5	5	Y	5	5	5	5	5	15	5.0	74	73	1	0	0	0	41	2.5
ROUTER-BRANCH-ATM [32]	5	5	Y	5	5	5	5	5	15	5.0	74	73	1	0	0	0	41	2.5
ROUTER [2]	5	5	Y	5	5	5	5	5	15	5.0	74	73	1	0	0	0	41	2.5
SERVERS - FILE AND PRINT [84]	5	5	Y	5	5	5	5	5	15	5.0	78	77	1	0	0	0	37	2.5
SMA OPCON [5]	5	5	Y	5	5	5	5	5	15	5.0	83	82	1	0	0	0	32	2.5
COGNOS [10]	5	5	Y	5	5	5	5	5	15	5.0	84	83	1	0	0	0	31	2.5
FISERV DIRECTOR [95]	5	5	Y	5	5	5	5	5	15	5.0	84	83	1	0	0	0	31	2.5
REAL VISION IMAGING [456]	5	5	Y	5	5	5	5	5	15	5.0	84	83	1	0	0	0	31	2.5
FED COMMAND [1]	5	5	Y	5	5	5	5	5	15	5.0	89	88	1	0	0	0	26	2.5
EMC SAN [2]	5	5	Y	5	5	5	5	5	15	5.0	94	93	1	0	0	0	21	2.5
DIRECT LINE WIRE [181]	5	5	Y	5	5	5	5	5	15	5.0	95	94	1	0	0	0	20	2.5
DIRECTLINE WIRE INTERNATIONAL [181]	5	5	Y	5	5	5	5	5	15	5.0	95	94	1	0	0	0	20	2.5
VERTEX [159]	5	5	Y	5	5	5	5	5	15	5.0	95	94	1	0	0	0	20	2.5
CASH MANAGEMENT ACH [166]	5	5	Y	5	5	5	5	5	15	5.0	102	101	1	0	0	0	13	2.5
CASH MANAGEMENT WIRE - DOMESTIC [70]	5	5	Y	5	5	5	5	5	15	5.0	102	101	1	0	0	0	13	2.5
SILVERLAKE [458]	5	5	Y	5	5	5	5	5	15	5.0	104	103	1	0	0	0	11	2.5
ISERIES [1]	5	5	Y	5	5	5	5	5	15	5.0	104	103	1	0	0	0	11	2.5
JHA 4|SIGHT [6]	5	5	Y	5	5	5	5	5	15	5.0	104	103	1	0	0	0	11	2.5
MICROSOFT EXCHANGE [2]	4	5	Y	5	5	5	5	4	14	5.0	78	77	1	0	0	0	37	2.5
CASH MANAGEMENT WIRE - INTERNATIONAL [13]	4	5	Y	5	5	5	5	4	14	5.0	102	101	1	0	0	0	13	2.5
CISCO CALL MANAGER SERVER [4]	5	3	N	5	4	3	4	4	11	4.0	75	74	1	0	0	0	40	2.0
CISCO UNITY VOICEMAIL SERVER [2]	5	3	N	5	4	3	4	4	11	4.0	75	74	1	0	0	0	40	2.0

Multiple Spreadsheets

jack henry & ASSOCIATES INC.

Why GRC Platform

Improve Business Resiliency

jack henry & ASSOCIATES INC.

Why GRC Platform

Mitigate Cyber Threats

jack henry & ASSOCIATES INC.

Why GRC Platform

Reduce Guesswork

jack henry & ASSOCIATES INC.

Why GRC Platform

Reduce Burden

jack henry & ASSOCIATES INC.

Why GRC Platform

Save Time

jack henry & ASSOCIATES INC.

Why GRC Platform

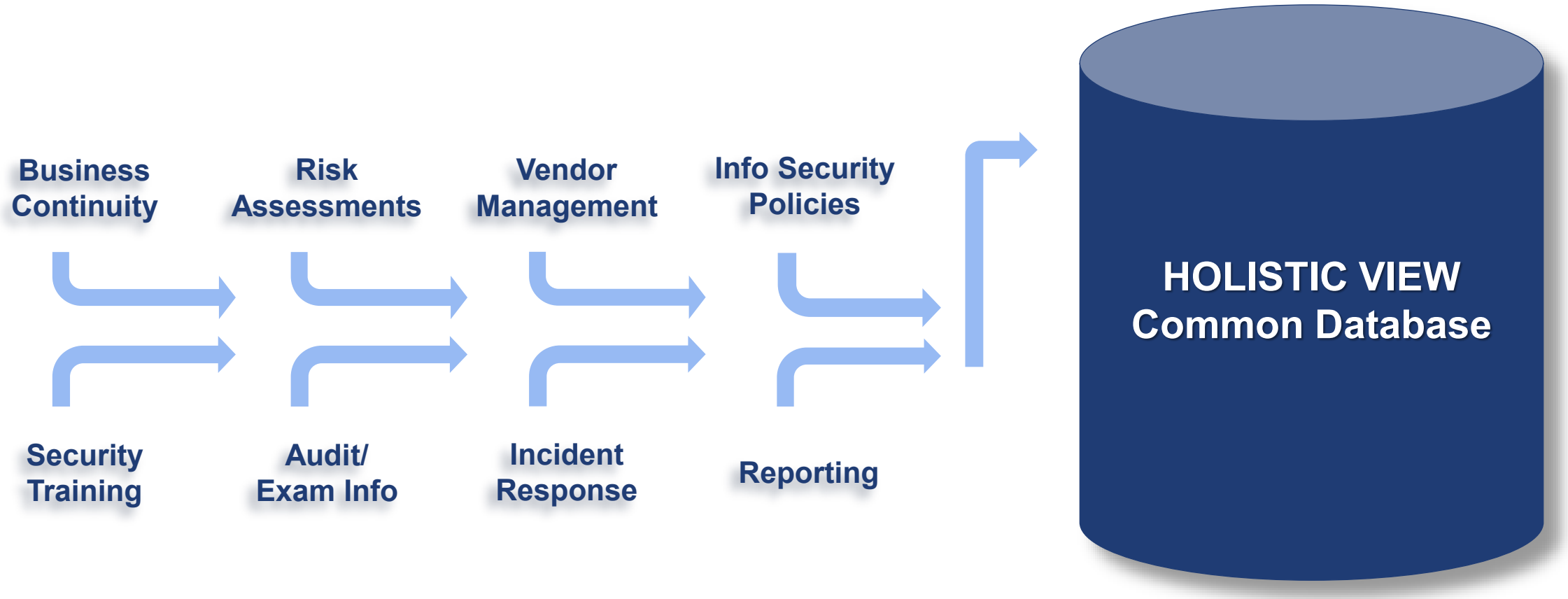
Save Money

jack henry & ASSOCIATES INC.

Why GRC Platform

Gain Efficiencies

GRC Automated



GRC in Action

- Asset Classification
- Risk Assessment
- Recovery Planning
- Vendor Management
- Policies

GRC in Action

- Asset Classification - helps prioritize the efforts to **assess** and **protect** information assets which are critical to business operations.

- Threats – helps identify high-risk assets to be protected.

GRC in Action

- Examples

Asset Types	Threats
✓ Server	✓ Natural
✓ Network	✓ Insider
✓ Storage	✓ External
✓ Office	✓ Technical
✓ Software	✓ Vendor/3rd Party
	✓ Cybersecurity

Saved: 9/8/2020 2:00 PM | Edit Record | Close

Asset Type	Asset Type: SERV/VM-Domain Controller	**Business Process**	
Environment	Production	**Asset Location**	
Asset Owner			
Asset Additional Info			
Asset Location Comments			
Asset Owner Comments			

Asset Classification

Location			
Transaction Volume	0 - Not Applicable	**Customer/Member Data**	Yes
Asset Criticality	5	**Confidential Data**	Yes
Data Sensitivity	5	**Internal Use Only Data**	Yes
Impact Score	5	**Impact Rating**	5 - Catastrophic

GRC in Action

- Risk and Control Categories – provides a unified approach to protect information assets critical to business operations.

- Risk Appetite – important to determine which and how much risk the Bank is willing to accept.

Content » Technology and Asset Repository » ABC Bank - ABC DC 1

Inherent Risk Evaluation

Inherent Risk Rating	4 - Major	**Count of Applicable Threats**	5
Overall Inherent Risk Score	19	**Sum of Inherent Risk Scores**	95

Related Controls

Count of Applicable Controls: 2

Related Organizational Control(s)

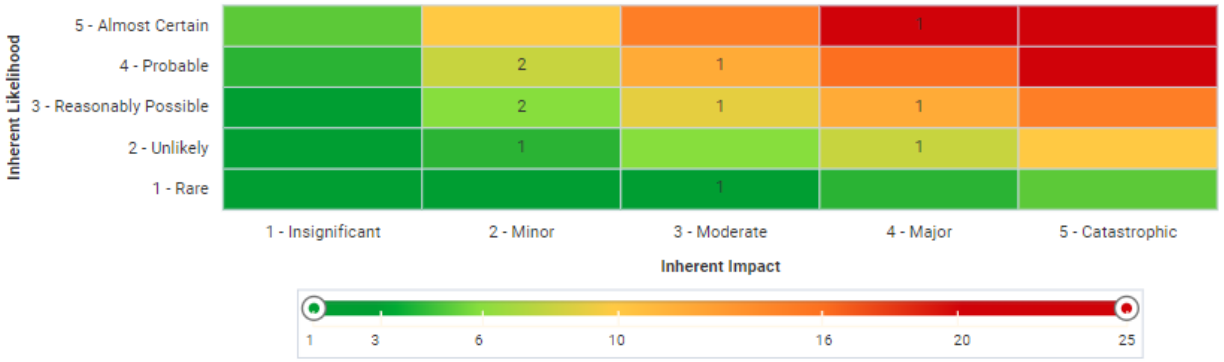
Control ID	Control Name	Owner	Control In Place?	Current Control Validation Score	Current Overall Control Rating
GC001 - Weyland-Yutani Corporation	Board Approved IS Policies		Yes	3	G - Partial 50% or Greater
AM001 – Access Controls	Role-Based Access		Yes	5	C - Effective with Comments

Residual Risk

Mitigation Score	0.68	**Residual Risk Score**	12.6
Risk Reduction Score	0.34	**Residual Risk Rating**	4 - Major

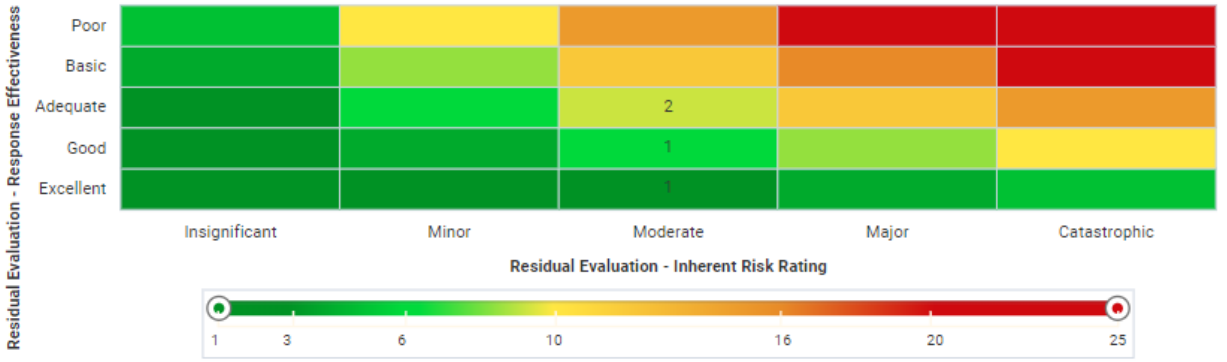
© 2020 Jack Henry & Associates, Inc.®

Inherent Risk Heat Map



Risk Id	Risk Category	Risk Title	Inherent Risk Rating	Current...	Inherent Persisten...	Inherent Velocity	Averag...
RISK-1	Financial IT	Data Breach	Major	12	4 - Enduring	2 - Average	12.58
RISK-2	Financial Operational Strategic	Employee Strike	Minor	3	3 - Moderate	1 - Slow	3
RISK-3	Reputational	Corporate Reputational Risk	Moderate	6	2 - Temporary	2 - Average	7.2
RISK-4	Financial Reputational	Financial Material Misstatement	Major	12	4 - Enduring	2 - Average	11.25
							Average: 9.03

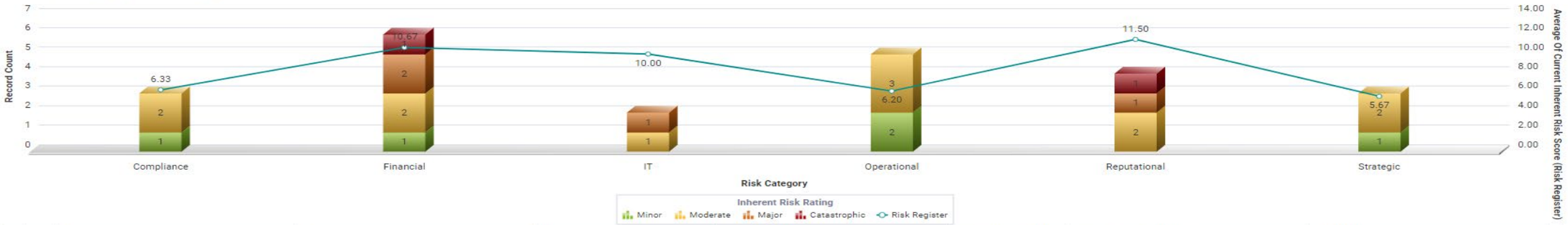
Residual Risk Heat Map



Risk Id	Risk Title	Risk Category	Last R...	Residual Evaluati...	Residual Evaluati...	Curren...	Curren...	Residual Risk Rat...
RISK-3	Corporate Reputational Risk	Reputational	2/5/2019	Moderate	Adequate	4.37	1	Minor
RISK-6	Business Continuity	Financial IT Operational	2/5/2019	Moderate	Good	5.13	1	Moderate
RISK-9	Ineffective Security Controls	Operational	2/6/2019	Moderate	Excellent	3.42	1	Minor
RISK-12	Risk of Financial Loss	Compliance Financial	2/1/2019	Moderate	Adequate	7.65	1	Moderate

4 items

Risks by Category and Average Score



Risk Title	Business Owner	Risk Category	Inherent Risk Rating	Current Inherent Ri...	Residual Impact Rating	Criticality
Money Laundering	Jason Rohlf	Financial Reputational	Catastrophic	20	2 - Minor	High
Financial Material Misstatement	Jason Rohlf	Financial Reputational	Major	12	3 - Moderate	Medium
Data Breach	Kyle Graves	Financial IT	Major	12	3 - Moderate	Medium

GRC in Action

- Recovery Planning – ensures response capabilities to safeguard employees, customers and business assets during a disruptive event.
- BIA (Business Impact Analysis) – should align with your risk appetite.

Content » Technology and Asset Repository » ABC Bank - ABC DC 1

Business Impact Analysis

Description	Domain Controllers		
Data Related?	No	**Recovery Point Objective (RPO)**	A=No Data Loss Acceptable
Recovery Time Capability (RTC)	0-4 hrs	**Maximum Allowable Downtime (MAD)**	4 hrs
Off Site Storage Locations		**Recovery Strategy**	Backup Equipment
Supplier(s)	Servers R Us	**Maintenance Provider(s)**	Gladiator Technology
Recovery Priority	2	**Recovery Sequence**	2
Business Impact Analysis	Servers-Domain Controller		
BIA Notes			

© 2020 Jack Henry & Associates, Inc.®

Content » Technology and Asset Repository » ABC Bank - ABC DC 1

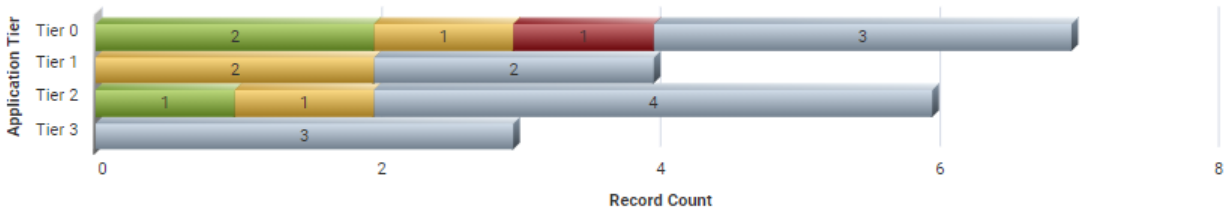
Business Continuity Plans

Recovery Plans

Title	Type	Plan Owner	Status	Related Incident Status
Oxford Hurricane Plan	Crisis Management	ABC Bank – Sara Lee	Compliant	No Open Incidents
Oxford Accounting BCP Plan	Crisis Management	ABC Bank – Sara Lee	Compliant	No Open Incidents

© 2020 Jack Henry & Associates, Inc.®

Applications by Tier and Plan Status

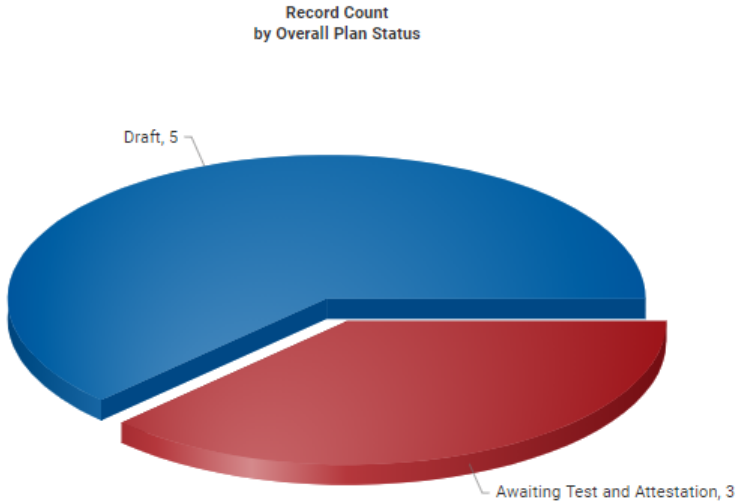


Recovery Plan Status
Compliant | In Review | Non-Compliant | No Active Plans

Name	Application Tier	Financially Significant	Recovery Plan Status
2901 Voice bundle PVDM3-16 UC license pac	Tier 2	No	No Active Plans
BIG-IP Virtual Ed Local Traffic Mgr Lic	Tier 1	No	In Review
BIG-IP Virtual Ed-Local Traffic Mgr Lic	Tier 1	No	No Active Plans
Client XYZ database host	Tier 0	Yes	Compliant
CMHPAVGDAW123456	Tier 3	No	No Active Plans

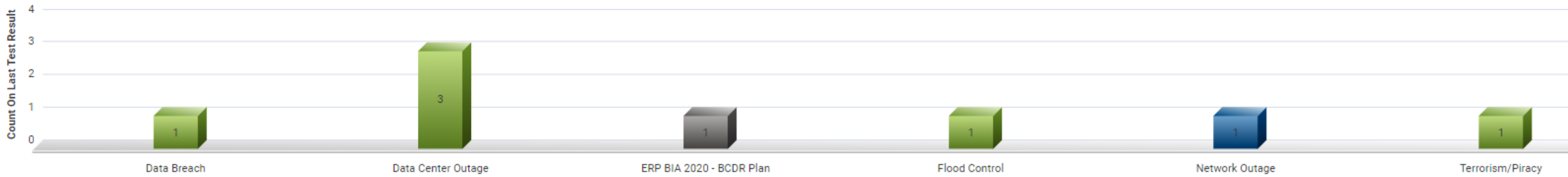
20 items

Continuity and Recovery Plans by Status



Total: 8

BCP Test Summary



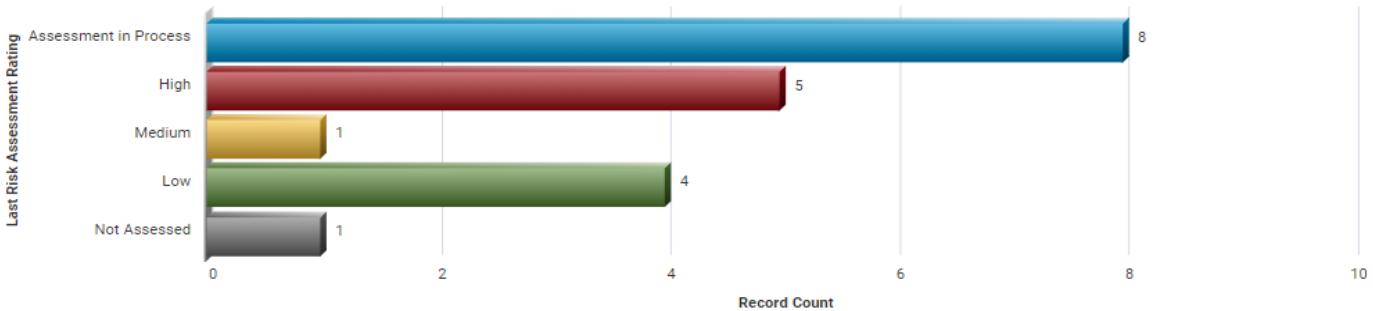
Last Test Result
Test In Process | Passed | No Tests Performed

Related Continuity and Recovery Plan	Title	Last Test Result	Last Test Date	Next Test Date
Data Breach	Wipe Device Data	Passed	1/12/2017	7/11/2017
Data Center Outage	Test and validate communications equipment	Passed	7/31/2018	8/30/2018
Data Center Outage	Back up and Recovery	Passed	7/31/2018	10/29/2018
Data Center Outage	Business continuity alert process	Passed	7/31/2018	10/29/2018

GRC in Action

- Vendor Management – provides visibility into your third party providers and their associated risks.

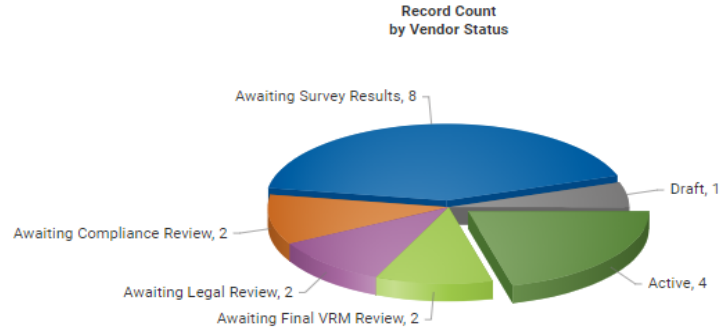
Vendors by Risk Assessment Rating



Vendor Name	Vendor Type	Relationship Owner	Spend - Tota...	Criticality Rating	Last Risk Assessment Rating
ABC Company	Consulting Services	Chris Pantaenius	$247,500	High	Low
ABC Hosting	Telecom and Networking	Kyle Graves	$2,250,000	High	Low
Calahan, Drake and Thompson	Business Services Legal	Chris Pantaenius	$0	High	Low
Cloudify	Software	Jason Rohlf	$0	High	Assessment in Process
Federal Reserve	Financial Services	Faith Wray	$0	High	Not Assessed
GRC Systems Inc.	Consulting Services	Jason Rohlf	$0	High	Assessment in Process
			Total: $11,772,500		

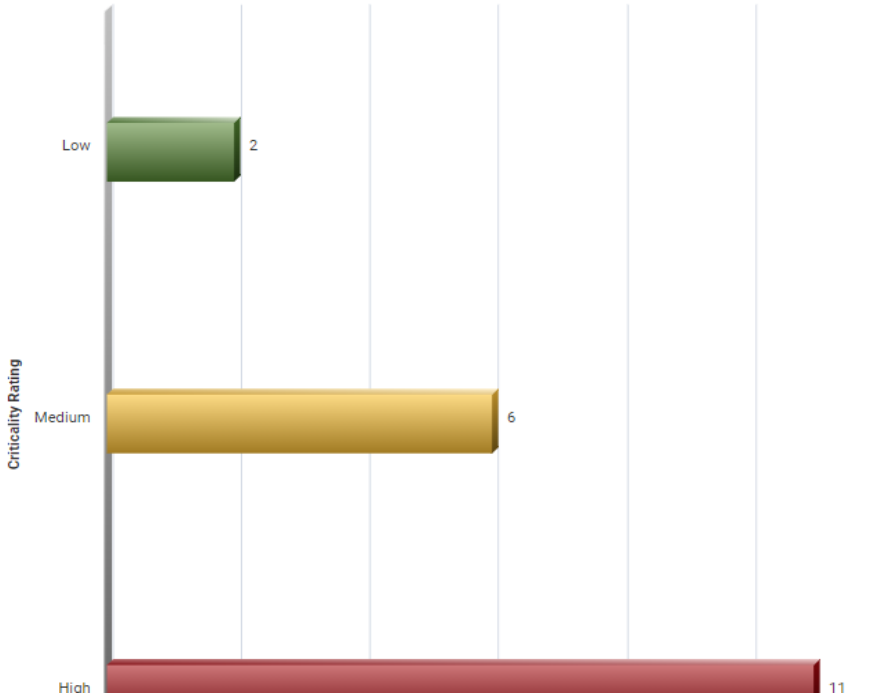
19 items

Vendors by Status

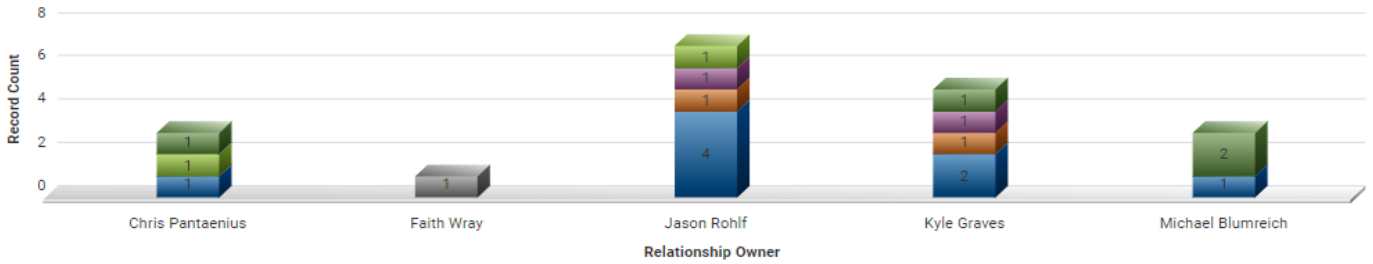


Total: 19

Vendors by Criticality

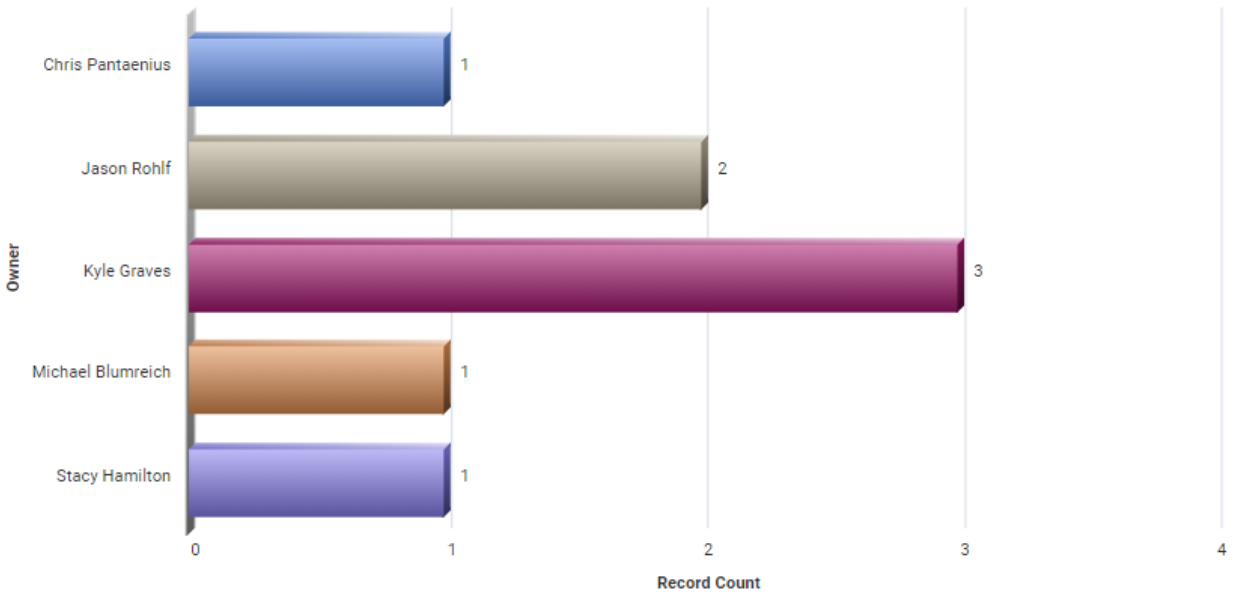


Vendors by Relationship Owner



Vendor Name	Relationship Owner	Vendor Status	Vendor Tier	Criticality Rating
ABC Company	Chris Pantaenius	Active	Tier 2	High
Calahan, Drake and Thompson	Chris Pantaenius	Awaiting Survey Results	Tier 3	High
InfoTech	Chris Pantaenius	Awaiting Final VRM Review	Tier 3	Medium

Policies by Owner



Pending Policy Reviews

Policy ID	Name	Owner	Review Status
001	Vendor Security Risk Management	Michael Blumreich	Awaiting Review
POL - 1900	Stored Cardholder Data Policy	Kyle Graves	Awaiting Review
TEST	Vendor Security Risk Management Standard	Jason Rohlf	Awaiting Review

3 items

Regulatory Changes Awaiting Review

UCF Authority Document	Change Date	Review Status
FFIEC IT Examination Handbook - Information Security	9/14/2017 9:20 AM	Open
FFIEC IT Examination Handbook - Management	9/14/2017 9:21 AM	Open
FFIEC IT Examination Handbook - Management	2/2/2018 1:09 PM	Open
FFIEC IT Examination Handbook - Management	2/2/2018 1:10 PM	Open
FFIEC IT Examination Handbook - Operations, July 2004	9/14/2017 9:21 AM	Open

Policies with Inactive Owners

Policy ID	Name	Statement	Category	Owner	Inactive Owner ...
001	Vendor Security Risk Management	Statement	Operations	Michael Blumreich	Inactive Owner
POL - 1100	Configuration Standards Policy	**Policy:** • A configuration standards document shall be created and maintained for each class of device that is installed into and/or connected directly to	Information Technology	Kyle Graves	Inactive Owner

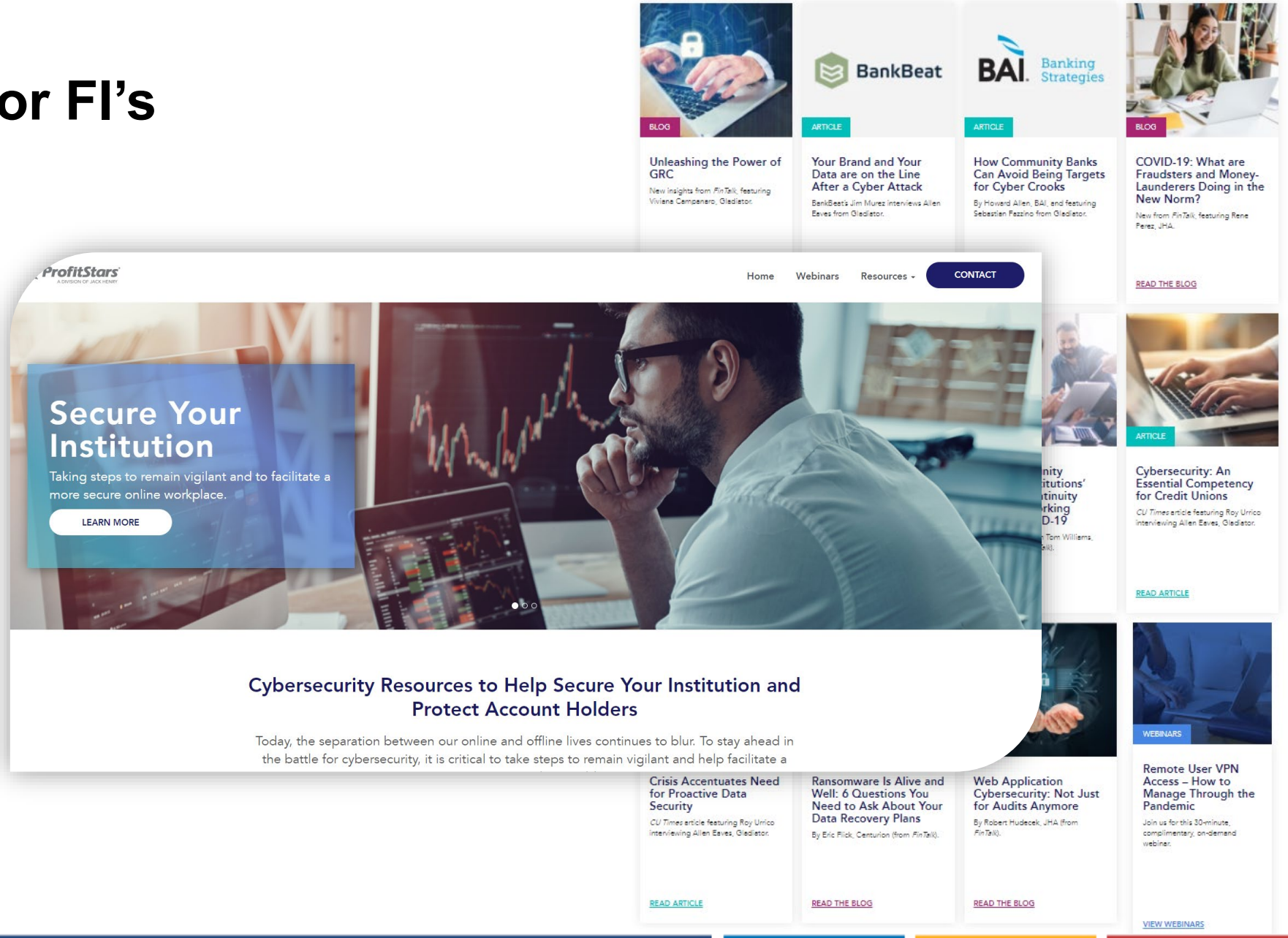
Where to Start?

- **In-House vs. Outsourced GRC platform**
  - Cost
  - Hardware & software fees
  - Implementation
  - Ongoing administration
  - Access to 3rd Party expertise
- **Internal Resources**
  - Risk Management Committee
  - Information Security/IT Steering
  - Communication
  - Integration

Resource Center for FI's

profitstars.com/cybersavvy

- Blogs
- Whitepapers
- Webinars
- Published articles
- Cybersecurity Forums



© 2020 Jack Henry & Associates, Inc.®

Gladiator™ IT Regulatory Compliance Services

- GRC SaaS Platform
- Virtual Information Security Officer
- InfoSec Asset Based Risk Assessment
- Written Information Security Policy
- Business Continuity Management
- Vendor Management
- Security Education Services

- "***Unleashing the Power of GRC"*** – Blog
  - https://discover.jackhenry.com/fintalk/unleashing-the-power-of-grc
- ***"Security Risk Assessments – A Balance of Risk and Controls"***
  - https://discover.jackhenry.com/fintalk/security-risk-assessments-a-balance-of-risk-and-controls

© 2020 Jack Henry & Associates, Inc.®

© 2020 Jack Henry & Associates, Inc.®