Risk & Control Management (RCMaaS)

APPLICATION DESCRIPTION

RiskCounts

“Confidential and Proprietary. Copyright (c) 2023 by RiskCounts. All Rights Reserved.”

Risk & Control Management Application

RiskCounts' **Risk & Control Management** application provides complete and standalone capability to conduct control effectiveness testing:

- Risk & Control Management is a major, and often mandatory, exercise by businesses to test the design of internal controls and controls effectiveness

- The focus is to ensure that controls are reducing the inherent risk to the extent that they have been designed for

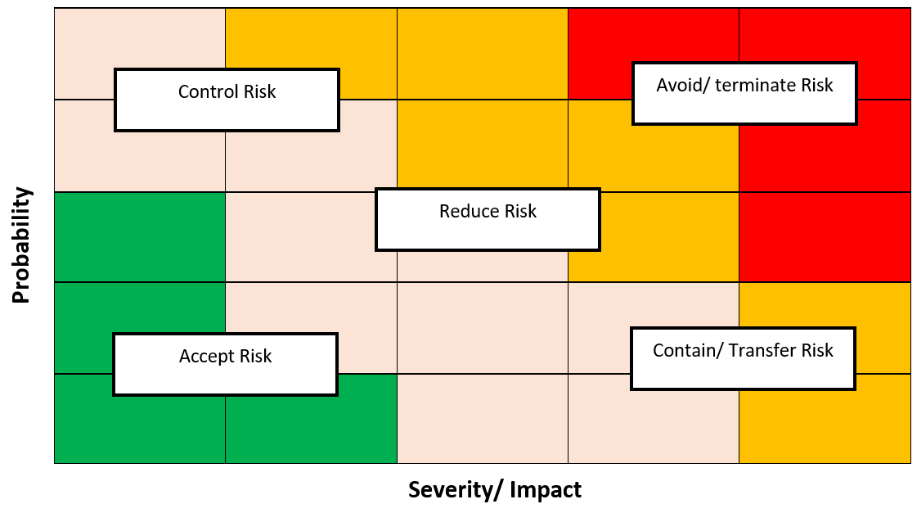
- RiskCounts provides a comprehensive RCMaaS Application, that:
  - allows organizations to conduct their quarterly risk-control reviews
  - offers simple workflow execution on a single platform
  - provides an inbuilt issue-tracking and remediation module; can be easily integrated with other issue and incident management systems that an organization may be using

"Confidential and Proprietary. Copyright (c) 2023 by RiskCounts. All Rights Reserved."

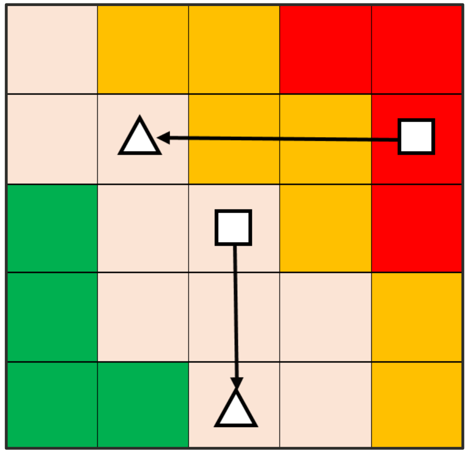
The Goal – Minimize Residual Risk: ascertain through Risk & Control Management (RCM)

Risk Control focus on response: the traditional “4 T’s” being Take, Transfer, Treat, or Terminate, where the areas in the Inherent Risk heatmap below relate to these actions, in a broad sense

□ Inherent Risk △ Residual Risk



Movement from Inherent to Residual levels is the effect of CONTROLS



- Residual Risk is of course “derived” as a fall-out, given the Inherent Risk Ratings and the Control Effectiveness
- Assessment is done through Risk Control Self-Assessment , and additionally informed by Events, Losses, Metrics, and Scenario Analysis.
- In other words, the Residual Risk is just the Inherent Risk discounted by, or adjusted for, the Control Assessment.
- Once scales are established, ALL risk-assessment should use the same calibration, whether Inherent or Residual.

“Confidential and Proprietary. Copyright (c) 2023 by RiskCounts. All Rights Reserved.”

Risk & Control Management (RCM) roles designation

There are four (4) key independent roles defined in RCM

Administrator

- Set up Risks
- Set up Policies
- Set up Control Categories
- Set up Control Procedures
- Set up Inherent Risk ratings

Risk Manager

- Set up Assessment Units (AUs) within organization
- Assign Risks and Assessors to AUs
- Initiate Self Assessment
- Finalize Risk Ratings based on inputs from AUs
- Collate and finalize all open Remediations & To-Dos: confirm ownership, dates and priority
- Reporting on rolled-up basis

Assessor

- Respond to simple 2-part questionnaire for each Control Category assigned for review.

Assessment Unit Coordinator

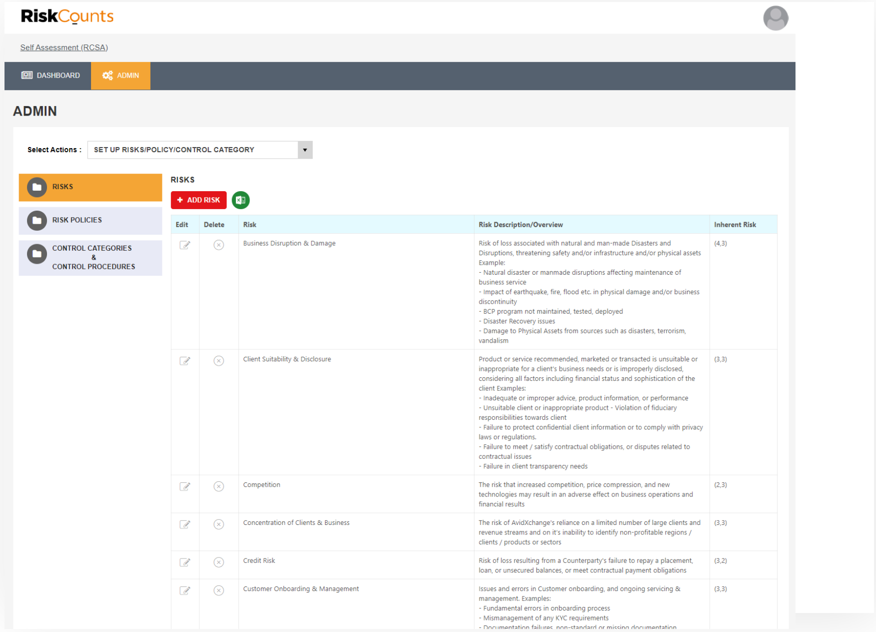
- Review Assessor scores for each Control Category
- Based on Assessor inputs, assign overall score for each Risk.
- Provide Remediation suggestions and drafts

"Confidential and Proprietary. Copyright (c) 2023 by RiskCounts. All Rights Reserved."

Set-up of Risk and Control Taxonomy and linking to policies

Define Risks

- Set up Risks and Risk descriptions in the library

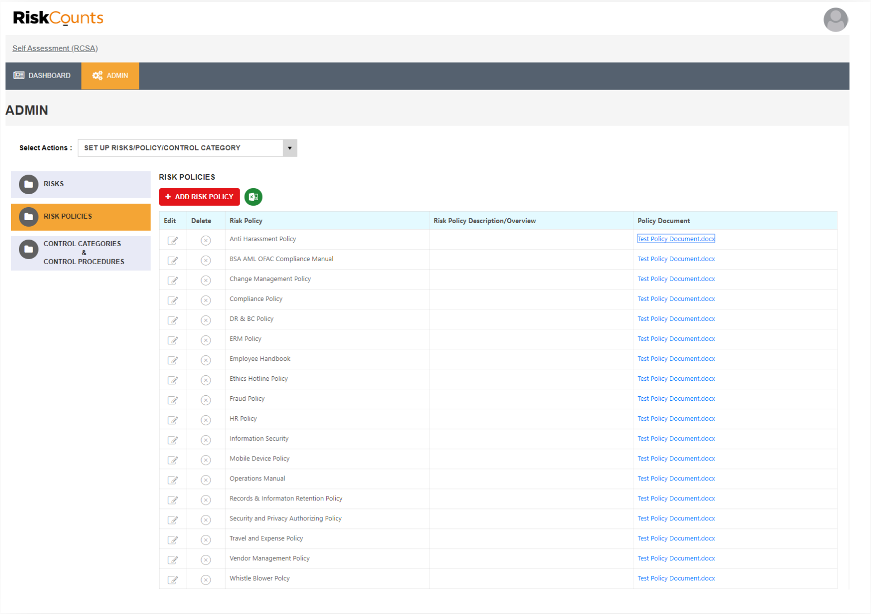


Select Actions : SET UP RISKS/POLICY/CONTROL CATEGORY

Edit	Delete	Risk	Risk Description/Overview	Inherent Risk
✎	⊗	Business Disruption & Damage	Risk of loss associated with natural and man-made Disasters and Disruptions, threatening safety and/or infrastructure and/or physical assets Example: - Natural disaster or manmade disruptions affecting maintenance of business service - Impact of earthquake, fire, flood etc. in physical damage and/or business discontinuity - BCP program not maintained, tested, deployed - Disaster Recovery issues - Damage to Physical Assets from sources such as disasters, terrorism, vandalism	(4,3)
✎	⊗	Client Suitability & Disclosure	Product or service recommended, marketed or transacted is unsuitable or inappropriate for a client's business needs or is improperly disclosed, considering all factors including financial status and sophistication of the client Examples: - Inadequate or improper advice, product information, or performance - Unsuitable client or inappropriate product - Violation of fiduciary responsibilities towards client - Failure to protect confidential client information or to comply with privacy laws or regulations. - Failure to meet / satisfy contractual obligations, or disputes related to contractual issues - Failure in client transparency needs	(3,3)
✎	⊗	Competition	The risk that increased competition, price compression, and new technologies may result in an adverse effect on business operations and financial results	(2,3)
✎	⊗	Concentration of Clients & Business	The risk of AvidXchange's reliance on a limited number of large clients and revenue streams and on it's inability to identify non-profitable regions / clients / products or sectors	(3,3)
✎	⊗	Credit Risk	Risk of loss resulting from a Counterparty's failure to repay a placement, loan, or unsecured balances, or meet contractual payment obligations	(3,2)
✎	⊗	Customer Onboarding & Management	Issues and errors in Customer onboarding, and ongoing servicing & management. Examples: - Fundamental errors in onboarding process - Mismanagement of any KYC requirements - Documentation failures, non-standard or missing documentation	(3,3)

Define Policies

- Set up Policies and Policy descriptions in the library
- Attach respective policy document



Select Actions : SET UP RISKS/POLICY/CONTROL CATEGORY

Edit	Delete	Risk Policy	Risk Policy Description/Overview	Policy Document
✎	⊗	Anti Harassment Policy		Test Policy Document.docx
✎	⊗	BSA AML OFAC Compliance Manual		Test Policy Document.docx
✎	⊗	Change Management Policy		Test Policy Document.docx
✎	⊗	Compliance Policy		Test Policy Document.docx
✎	⊗	DR & BC Policy		Test Policy Document.docx
✎	⊗	ERM Policy		Test Policy Document.docx
✎	⊗	Employee Handbook		Test Policy Document.docx
✎	⊗	Ethics Hotline Policy		Test Policy Document.docx
✎	⊗	Fraud Policy		Test Policy Document.docx
✎	⊗	HR Policy		Test Policy Document.docx
✎	⊗	Information Security		Test Policy Document.docx
✎	⊗	Mobile Device Policy		Test Policy Document.docx
✎	⊗	Operations Manual		Test Policy Document.docx
✎	⊗	Records & Informaton Retention Policy		Test Policy Document.docx
✎	⊗	Security and Privacy Authorizing Policy		Test Policy Document.docx
✎	⊗	Travel and Expense Policy		Test Policy Document.docx
✎	⊗	Vendor Management Policy		Test Policy Document.docx
✎	⊗	Whistle Blower Polcy		Test Policy Document.docx

Administrator
Assessor
Assessment Unit Coordinator
Risk Manager

"Confidential and Proprietary. Copyright (c) 2023 by RiskCounts. All Rights Reserved."

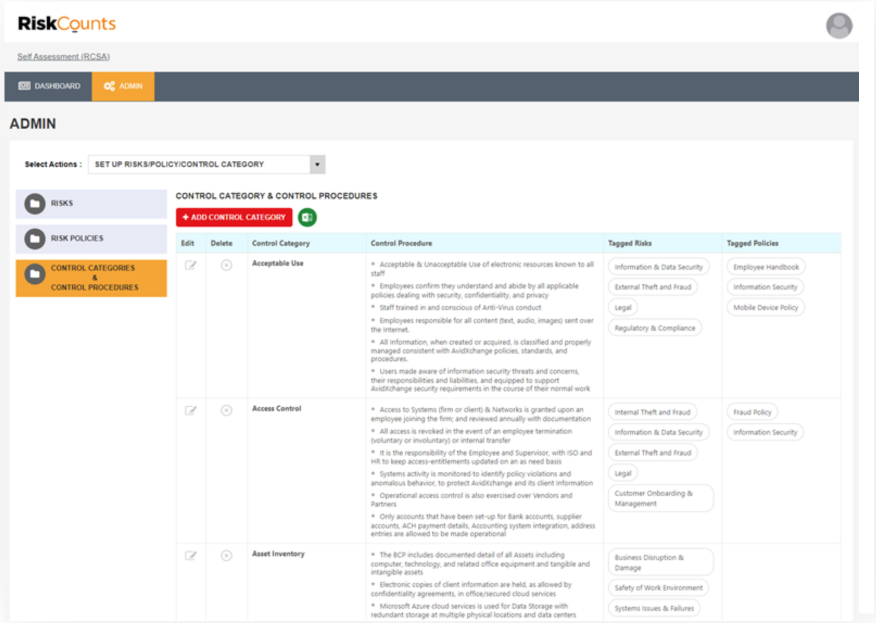
Inherent Risk set-up and assessment

Define Control Categories

- Set up Control Categories and Procedures in the library
- Tag associated Risks
- Tag Associated Policies

Assign Inherent Risk ratings

- Assign an Inherent Risk rating for each Risk, based on Severity and Likelihood of events
- Severity & Likelihood scales provided alongside are based on Financial loss definitions specific to each organization



RiskCounts

Self Assessment (RCSA)

DASHBOARD | ADMIN

ADMIN

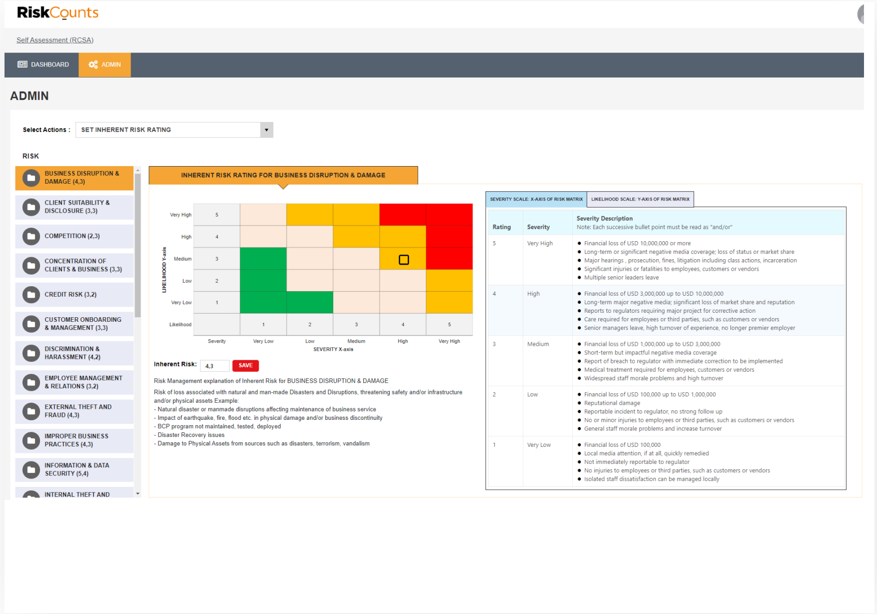
Select Actions : SET UP RISKS/POLICY/CONTROL CATEGORY

- RISKS
- RISK POLICIES
- CONTROL CATEGORIES & CONTROL PROCEDURES

CONTROL CATEGORY & CONTROL PROCEDURES

+ ADD CONTROL CATEGORY

Edit	Delete	Control Category	Control Procedure	Tagged Risks	Tagged Policies
		Acceptable Use	* Acceptable & Unacceptable Use of electronic resources known to all staff * Employees confirm they understand and abide by all applicable policies dealing with security, confidentiality, and privacy * Staff trained in and conscious of Anti-Virus conduct * Employees responsible for all content (text, audio, images) sent over the Internet. * All Information, when created or acquired, is classified and properly managed consistent with AvidXchange policies, standards, and procedures. * Users made aware of information security threats and concerns, their responsibilities and liabilities, and equipped to support AvidXchange security requirements in the course of their normal work	Information & Data Security External Theft and Fraud Legal Regulatory & Compliance	Employee Handbook Information Security Mobile Device Policy
		Access Control	* Access to Systems (firm or client) & Networks is granted upon an employee joining the firm; and reviewed annually with documentation * All access is revoked in the event of an employee termination (voluntary or involuntary) or internal transfer * It is the responsibility of the Employee and Supervisor, with ISO and HR to keep access-entitlements updated on an as need basis * Systems activity is monitored to identify policy violations and anomalous behavior, to protect AvidXchange and its client information * Operational access control is also exercised over Vendors and Partners * Only accounts that have been set-up for Bank accounts, supplier accounts, ACH payment details, Accounting system integration, address entries are allowed to be made operational	Internal Theft and Fraud Information & Data Security External Theft and Fraud Legal Customer Onboarding & Management	Fraud Policy Information Security
		Asset Inventory	* The BCP includes documented detail of all Assets including computer, technology, and related office equipment and tangible and intangible assets * Electronic copies of client information are held, as allowed by confidentiality agreements, in office/secured cloud services * Microsoft Azure cloud services is used for Data Storage with redundant storage at multiple physical locations and data centers	Business Disruption & Damage Safety of Work Environment Systems Issues & Failures	



RiskCounts

Self Assessment (RCSA)

DASHBOARD | ADMIN

ADMIN

Select Actions : SET INHERENT RISK RATING

RISK

- BUSINESS DISRUPTION & DAMAGE (4,3)
- CLIENT SUITABILITY & DISCLOSURE (3,3)
- COMPETITION (2,3)
- CONCENTRATION OF CLIENTS & BUSINESS (3,3)
- CREDIT RISK (3,2)
- CUSTOMER ONBOARDING & MANAGEMENT (3,3)
- DISCRIMINATION & HARASSMENT (4,2)
- EMPLOYEE MANAGEMENT & RELATIONS (3,2)
- EXTERNAL THEFT AND FRAUD (4,3)
- IMPROPER BUSINESS PRACTICES (4,3)
- INFORMATION & DATA SECURITY (5,4)
- INTERNAL THEFT AND

INHERENT RISK RATING FOR BUSINESS DISRUPTION & DAMAGE

LIKELIHOOD Y-axis

Very High	5	⬜	🟨	🟨	🟥	🟥
High	4	⬜	⬜	🟨	🟨	🟥
Medium	3	🟩	⬜	⬜	🟨 □	🟥
Low	2	🟩	⬜	⬜	⬜	🟨
Very Low	1	🟩	🟩	⬜	⬜	🟨
Likelihood		1	2	3	4	5
	Severity	Very Low	Low	Medium	High	Very High

SEVERITY X-axis

Inherent Risk: 4,3 SAVE

Risk Management explanation of Inherent Risk for BUSINESS DISRUPTION & DAMAGE

Risk of loss associated with natural and man-made Disasters and Disruptions, threatening safety and/or infrastructure and/or physical assets Example:
- Natural disaster or manmade disruptions affecting maintenance of business service
- Impact of earthquake, fire, flood etc. in physical damage and/or business discontinuity
- BCP program not maintained, tested, deployed
- Disaster Recovery issues
- Damage to Physical Assets from sources such as disasters, terrorism, vandalism

SEVERITY SCALE: X-AXIS OF RISK MATRIX | LIKELIHOOD SCALE: Y-AXIS OF RISK MATRIX

Rating	Severity	Severity Description Note: Each successive bullet point must be read as "and/or"
5	Very High	● Financial loss of USD 10,000,000 or more ● Long-term or significant negative media coverage; loss of status or market share ● Major hearings , prosecution, fines, litigation including class actions, incarceration ● Significant injuries or fatalities to employees, customers or vendors ● Multiple senior leaders leave
4	High	● Financial loss of USD 3,000,000 up to USD 10,000,000 ● Long-term major negative media; significant loss of market share and reputation ● Reports to regulators requiring major project for corrective action ● Care required for employees or third parties, such as customers or vendors ● Senior managers leave, high turnover of experience, no longer premier employer
3	Medium	● Financial loss of USD 1,000,000 up to USD 3,000,000 ● Short-term but impactful negative media coverage ● Report of breach to regulator with immediate correction to be implemented ● Medical treatment required for employees, customers or vendors ● Widespread staff morale problems and high turnover
2	Low	● Financial loss of USD 100,000 up to USD 1,000,000 ● Reputational damage ● Reportable incident to regulator, no strong follow up ● No or minor injuries to employees or third parties, such as customers or vendors ● General staff morale problems and increase turnover
1	Very Low	● Financial loss of USD 100,000 ● Local media attention, if at all, quickly remedied ● Not immediately reportable to regulator ● No injuries to employees or third parties, such as customers or vendors ● Isolated staff dissatisfaction can be managed locally

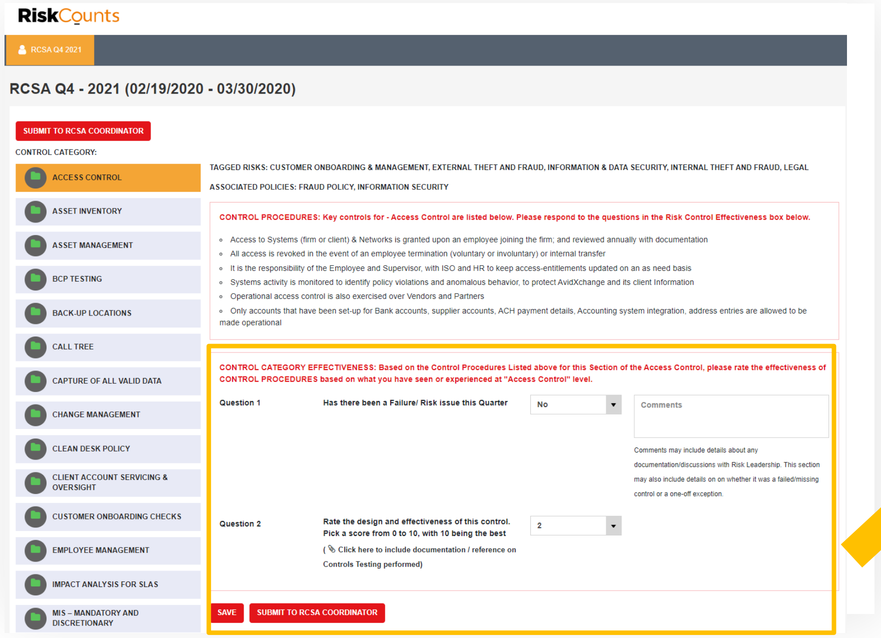
Administrator → Assessor → Assessment Unit Coordinator → Risk Manager

"Confidential and Proprietary. Copyright (c) 2023 by RiskCounts. All Rights Reserved."

Control Assessment

Assessment

- Assessors respond to a 2-part questionnaire as part of review
- Attach documentary evidence as specified by the firm



RCSA Q4 - 2021 (02/19/2020 - 03/30/2020)

CONTROL CATEGORY:

TAGGED RISKS: CUSTOMER ONBOARDING & MANAGEMENT, EXTERNAL THEFT AND FRAUD, INFORMATION & DATA SECURITY, INTERNAL THEFT AND FRAUD, LEGAL

ASSOCIATED POLICIES: FRAUD POLICY, INFORMATION SECURITY

CONTROL PROCEDURES: Key controls for - Access Control are listed below. Please respond to the questions in the Risk Control Effectiveness box below.

- Access to Systems (firm or client) & Networks is granted upon an employee joining the firm; and reviewed annually with documentation
- All access is revoked in the event of an employee termination (voluntary or involuntary) or internal transfer
- It is the responsibility of the Employee and Supervisor, with ISO and HR to keep access-entitlements updated on an as need basis
- Systems activity is monitored to identify policy violations and anomalous behavior, to protect AvidXchange and its client Information
- Operational access control is also exercised over Vendors and Partners
- Only accounts that have been set-up for Bank accounts, supplier accounts, ACH payment details, Accounting system integration, address entries are allowed to be made operational

CONTROL CATEGORY EFFECTIVENESS: Based on the Control Procedures Listed above for this Section of the Access Control, please rate the effectiveness of CONTROL PROCEDURES based on what you have seen or experienced at "Access Control" level.

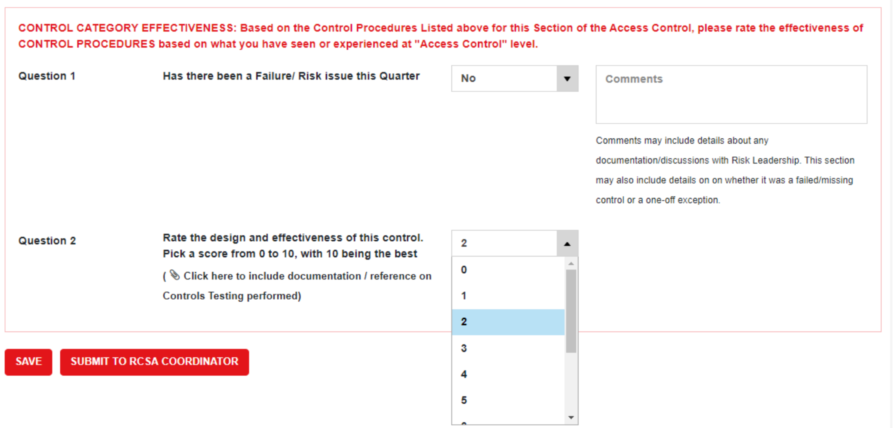
Question 1 Has there been a Failure/ Risk issue this Quarter: No

Comments

Comments may include details about any documentation/discussions with Risk Leadership. This section may also include details on on whether it was a failed/missing control or a one-off exception.

Question 2 Rate the design and effectiveness of this control. Pick a score from 0 to 10, with 10 being the best: 2

(📎 Click here to include documentation / reference on Controls Testing performed)



CONTROL CATEGORY EFFECTIVENESS: Based on the Control Procedures Listed above for this Section of the Access Control, please rate the effectiveness of CONTROL PROCEDURES based on what you have seen or experienced at "Access Control" level.

Question 1 Has there been a Failure/ Risk issue this Quarter: No

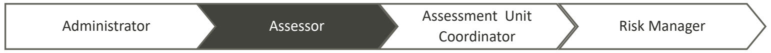
Comments

Comments may include details about any documentation/discussions with Risk Leadership. This section may also include details on on whether it was a failed/missing control or a one-off exception.

Question 2 Rate the design and effectiveness of this control. Pick a score from 0 to 10, with 10 being the best: 2

(📎 Click here to include documentation / reference on Controls Testing performed)

RiskCounts



“Confidential and Proprietary. Copyright (c) 2023 by RiskCounts. All Rights Reserved.”

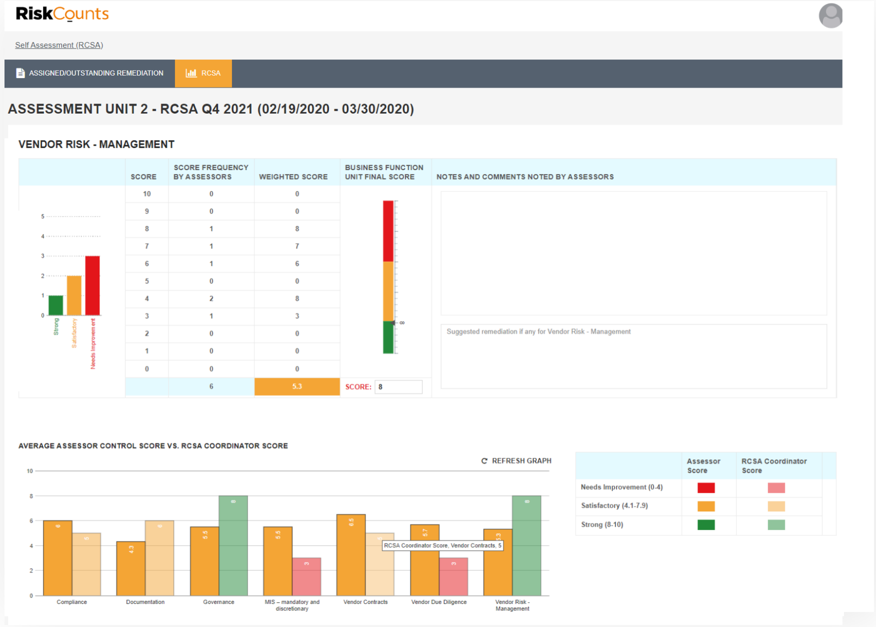
Review of assessments and Issue Management

Consolidation

- Review and consolidate Assessor scores into an overall score for each Risk
- Provide Remediation drafts for each Control Category

Remediation Resolution

- Review, Resolve and Update assigned Remediations for Control Categories



RiskCounts

Self Assessment (RCSA)

ASSIGNED/OUTSTANDING REMEDIATION | RCSA

ASSESSMENT UNIT 2 - RCSA Q4 2021 (02/19/2020 - 03/30/2020)

VENDOR RISK - MANAGEMENT

SCORE	SCORE FREQUENCY BY ASSESSORS	WEIGHTED SCORE
10	0	0
9	0	0
8	1	8
7	1	7
6	1	6
5	0	0
4	2	8
3	1	3
2	0	0
1	0	0
0	0	0
	6	5.3

BUSINESS FUNCTION UNIT FINAL SCORE

SCORE: 8

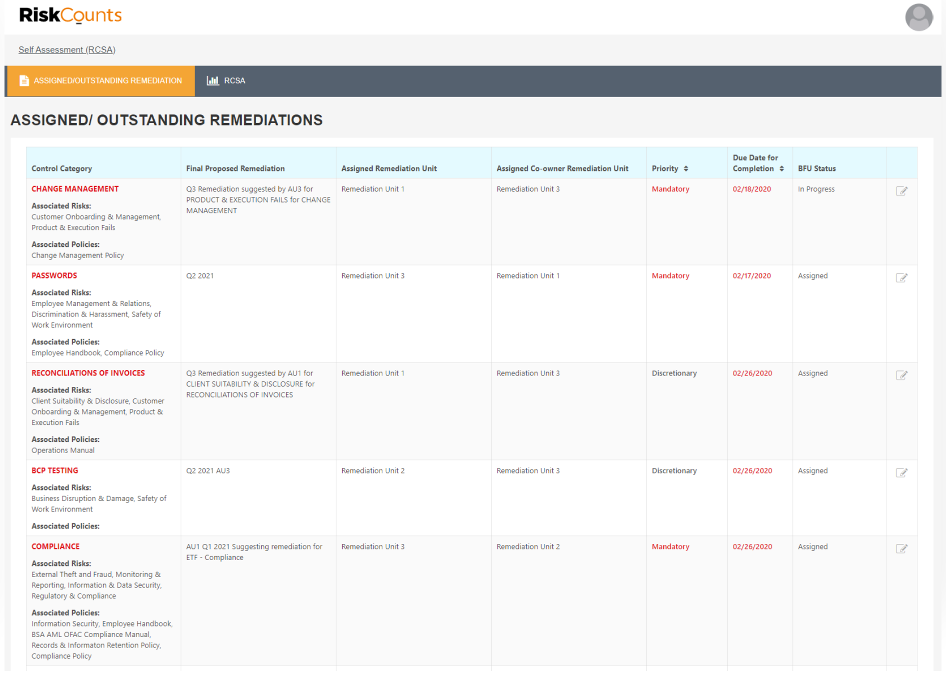
NOTES AND COMMENTS NOTED BY ASSESSORS

Suggested remediation if any for Vendor Risk - Management

AVERAGE ASSESSOR CONTROL SCORE VS. RCSA COORDINATOR SCORE

REFRESH GRAPH

	Assessor Score	RCSA Coordinator Score
Needs Improvement (0-4)	🟥	🟥
Satisfactory (4.1-7.9)	🟧	🟧
Strong (8-10)	🟩	🟩



RiskCounts

Self Assessment (RCSA)

ASSIGNED/OUTSTANDING REMEDIATION | RCSA

ASSIGNED/ OUTSTANDING REMEDIATIONS

Control Category	Final Proposed Remediation	Assigned Remediation Unit	Assigned Co-owner Remediation Unit	Priority ⇕	Due Date for Completion ⇕	BFU Status	
CHANGE MANAGEMENT **Associated Risks:** Customer Onboarding & Management, Product & Execution Fails **Associated Policies:** Change Management Policy	Q3 Remediation suggested by AU3 for PRODUCT & EXECUTION FAILS for CHANGE MANAGEMENT	Remediation Unit 1	Remediation Unit 3	Mandatory	02/18/2020	In Progress	✎
PASSWORDS **Associated Risks:** Employee Management & Relations, Discrimination & Harassment, Safety of Work Environment **Associated Policies:** Employee Handbook, Compliance Policy	Q2 2021	Remediation Unit 3	Remediation Unit 1	Mandatory	02/17/2020	Assigned	✎
RECONCILIATIONS OF INVOICES **Associated Risks:** Client Suitability & Disclosure, Customer Onboarding & Management, Product & Execution Fails **Associated Policies:** Operations Manual	Q3 Remediation suggested by AU1 for CLIENT SUITABILITY & DISCLOSURE for RECONCILIATIONS OF INVOICES	Remediation Unit 1	Remediation Unit 3	Discretionary	02/26/2020	Assigned	✎
BCP TESTING **Associated Risks:** Business Disruption & Damage, Safety of Work Environment **Associated Policies:**	Q2 2021 AU3	Remediation Unit 2	Remediation Unit 3	Discretionary	02/26/2020	Assigned	✎
COMPLIANCE **Associated Risks:** External Theft and Fraud, Monitoring & Reporting, Information & Data Security, Regulatory & Compliance **Associated Policies:** Information Security, Employee Handbook, BSA AML OFAC Compliance Manual, Records & Informaton Retention Policy, Compliance Policy	AU1 Q1 2021 Suggesting remediation for ETF - Compliance	Remediation Unit 3	Remediation Unit 2	Mandatory	02/26/2020	Assigned	✎

RiskCounts

Administrator

Assessor

Assessment Unit Coordinator

Risk Manager

“Confidential and Proprietary. Copyright (c) 2023 by RiskCounts. All Rights Reserved.”

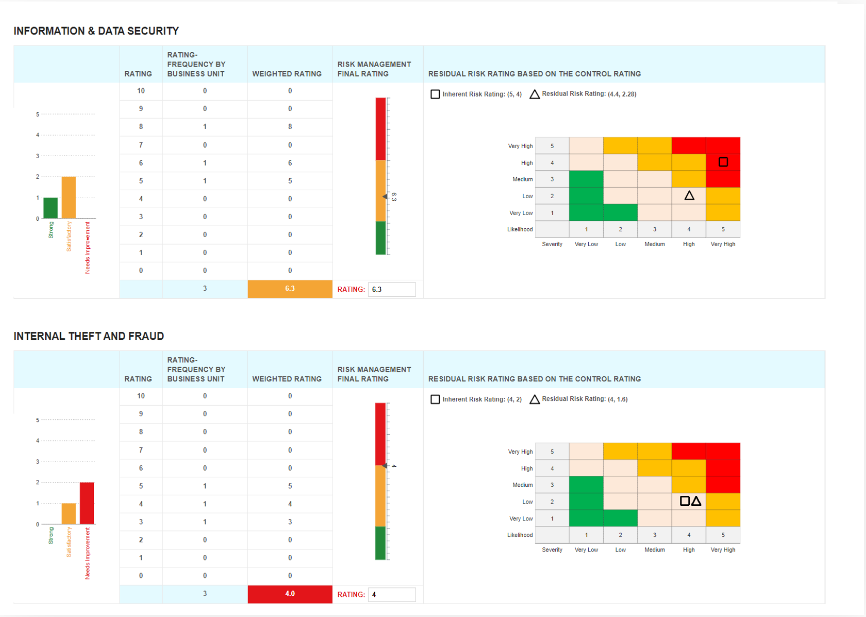
Consolidated Risk view (Inherent & Residual Risk)

Consolidate Risk Ratings

- Initiate Self Assessment
- Manage RCM process
- Consolidate Risk scores from Assessment Units into Risk Rating to arrive at Residual Risk Rating.

Remediation Management

- Review suggested Remediations
- Assign & Manage Remediations within the application



INFORMATION & DATA SECURITY

RATING	RATING-FREQUENCY BY BUSINESS UNIT	WEIGHTED RATING
10	0	0
9	0	0
8	1	8
7	0	0
6	1	6
5	1	5
4	0	0
3	0	0
2	0	0
1	0	0
0	0	0
	3	6.3

RISK MANAGEMENT FINAL RATING

RATING: 6.3

RESIDUAL RISK RATING BASED ON THE CONTROL RATING

□ Inherent Risk Rating: (5, 4) △ Residual Risk Rating: (4.4, 2.28)

Very High	5					
High	4					□
Medium	3					
Low	2				△	
Very Low	1					
Likelihood		1	2	3	4	5
	Severity	Very Low	Low	Medium	High	Very High

INTERNAL THEFT AND FRAUD

RATING	RATING-FREQUENCY BY BUSINESS UNIT	WEIGHTED RATING
10	0	0
9	0	0
8	0	0
7	0	0
6	0	0
5	1	5
4	1	4
3	1	3
2	0	0
1	0	0
0	0	0
	3	4.0

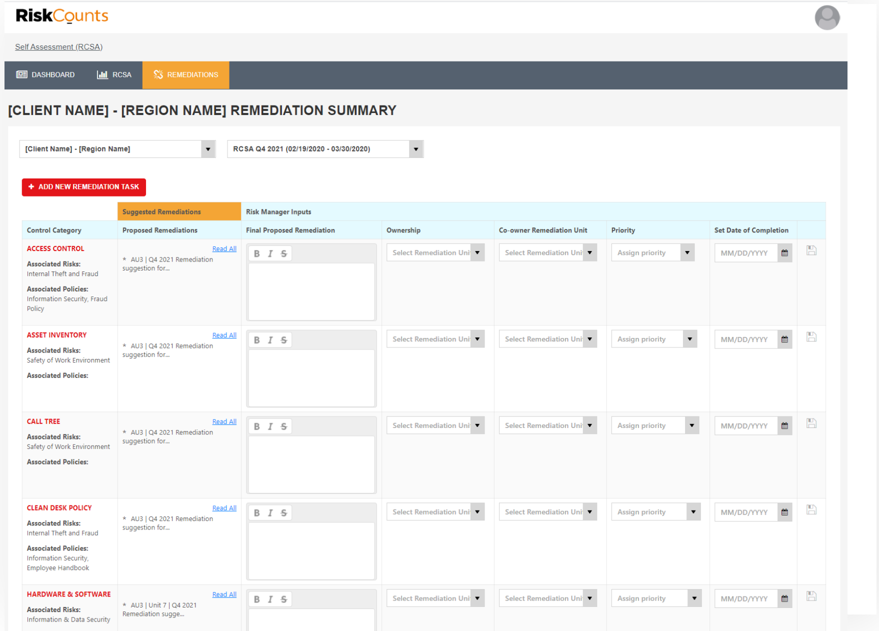
RISK MANAGEMENT FINAL RATING

RATING: 4

RESIDUAL RISK RATING BASED ON THE CONTROL RATING

□ Inherent Risk Rating: (4, 2) △ Residual Risk Rating: (4, 1.6)

Very High	5					
High	4					
Medium	3					
Low	2				□△	
Very Low	1					
Likelihood		1	2	3	4	5
	Severity	Very Low	Low	Medium	High	Very High



RiskCounts

Self Assessment (RCSA)

[CLIENT NAME] - [REGION NAME] REMEDIATION SUMMARY

[Client Name] - [Region Name]

RCSA Q4 2021 (02/19/2020 - 03/30/2020)

	Suggested Remediations	Risk Manager Inputs				
Control Category	Proposed Remediations	Final Proposed Remediation	Ownership	Co-owner Remediation Unit	Priority	Set Date of Completion
ACCESS CONTROL Associated Risks: Internal Theft and Fraud Associated Policies: Information Security, Fraud Policy	Read All * AU3 | Q4 2021 Remediation suggestion for...	B I S	Select Remediation Uni	Select Remediation Uni	Assign priority	MM/DD/YYYY
ASSET INVENTORY Associated Risks: Safety of Work Environment Associated Policies:	Read All * AU3 | Q4 2021 Remediation suggestion for...	B I S	Select Remediation Uni	Select Remediation Uni	Assign priority	MM/DD/YYYY
CALL TREE Associated Risks: Safety of Work Environment Associated Policies:	Read All * AU3 | Q4 2021 Remediation suggestion for...	B I S	Select Remediation Uni	Select Remediation Uni	Assign priority	MM/DD/YYYY
CLEAN DESK POLICY Associated Risks: Internal Theft and Fraud Associated Policies: Information Security, Employee Handbook	Read All * AU3 | Q4 2021 Remediation suggestion for...	B I S	Select Remediation Uni	Select Remediation Uni	Assign priority	MM/DD/YYYY
HARDWARE & SOFTWARE Associated Risks: Information & Data Security	Read All * AU3 | Unit 7 | Q4 2021 Remediation sugge...	B I S	Select Remediation Uni	Select Remediation Uni	Assign priority	MM/DD/YYYY

RiskCounts

Administrator

Assessor

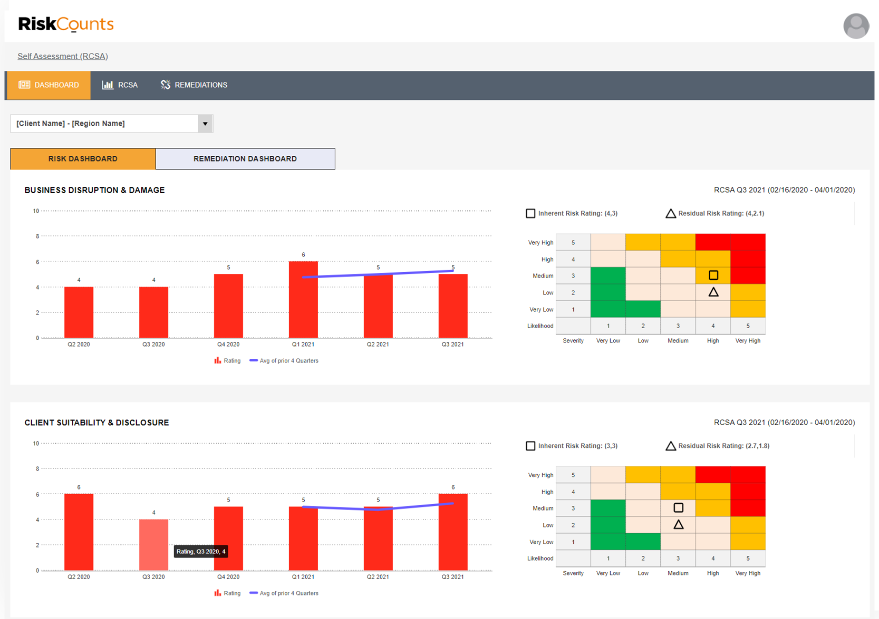
Assessment Unit Coordinator

Risk Manager

Management Dashboard

Risk Dashboard

- Displays Rating trends for each Risk within organization
- Displays Inherent Risk rating and Residual Risk Rating on Heatmap for the latest RCM



[Client Name] - [Region Name]

BUSINESS DISRUPTION & DAMAGE

RCSA Q3 2021 (02/16/2020 - 04/01/2020)

Q2 2020	Q3 2020	Q4 2020	Q1 2021	Q2 2021	Q3 2021
4	4	5	6	5	5

□ Inherent Risk Rating: (4,3) △ Residual Risk Rating: (4,2.1)

Very High	5	⬜	🟨	🟨	🟥	🟥
High	4	⬜	⬜	🟨	🟨	🟥
Medium	3	🟩	⬜	⬜	🟨 □	🟥
Low	2	🟩	⬜	⬜	⬜ △	🟨
Very Low	1	🟩	🟩	⬜	⬜	🟨
Likelihood		1	2	3	4	5
	Severity	Very Low	Low	Medium	High	Very High

CLIENT SUITABILITY & DISCLOSURE

RCSA Q3 2021 (02/16/2020 - 04/01/2020)

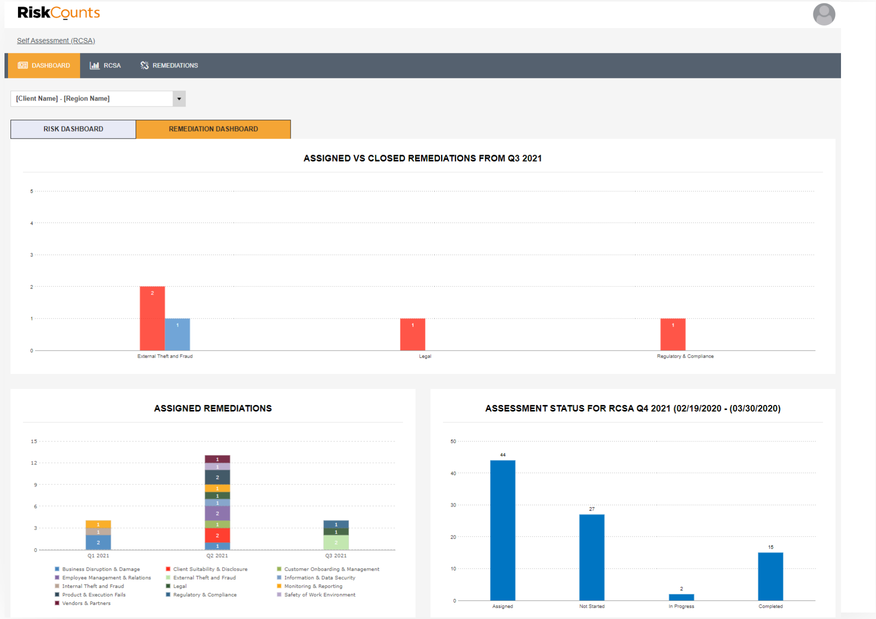
Q2 2020	Q3 2020	Q4 2020	Q1 2021	Q2 2021	Q3 2021
6	4	5	5	5	6

□ Inherent Risk Rating: (3,3) △ Residual Risk Rating: (2.7,1.8)

Very High	5	⬜	🟨	🟨	🟥	🟥
High	4	⬜	⬜	🟨	🟨	🟥
Medium	3	🟩	⬜	⬜ □	🟨	🟥
Low	2	🟩	⬜	⬜ △	⬜	🟨
Very Low	1	🟩	🟩	⬜	⬜	🟨
Likelihood		1	2	3	4	5
	Severity	Very Low	Low	Medium	High	Very High

Remediation Dashboard

- Displays chart for outstanding vs closed remediation for previous quarter
- Assigned remediations for last 4 quarters
- Response status of Assessors for ongoing Self Assessment



[Client Name] - [Region Name]

ASSIGNED VS CLOSED REMEDIATIONS FROM Q3 2021

ASSIGNED REMEDIATIONS

ASSESSMENT STATUS FOR RCSA Q4 2021 (02/19/2020 - (03/30/2020)

Assigned	Not Started	In Progress	Completed
44	27	2	15

RiskCounts

Administrator → Assessor → Assessment Unit Coordinator → Risk Manager

“Confidential and Proprietary. Copyright (c) 2023 by RiskCounts. All Rights Reserved.”