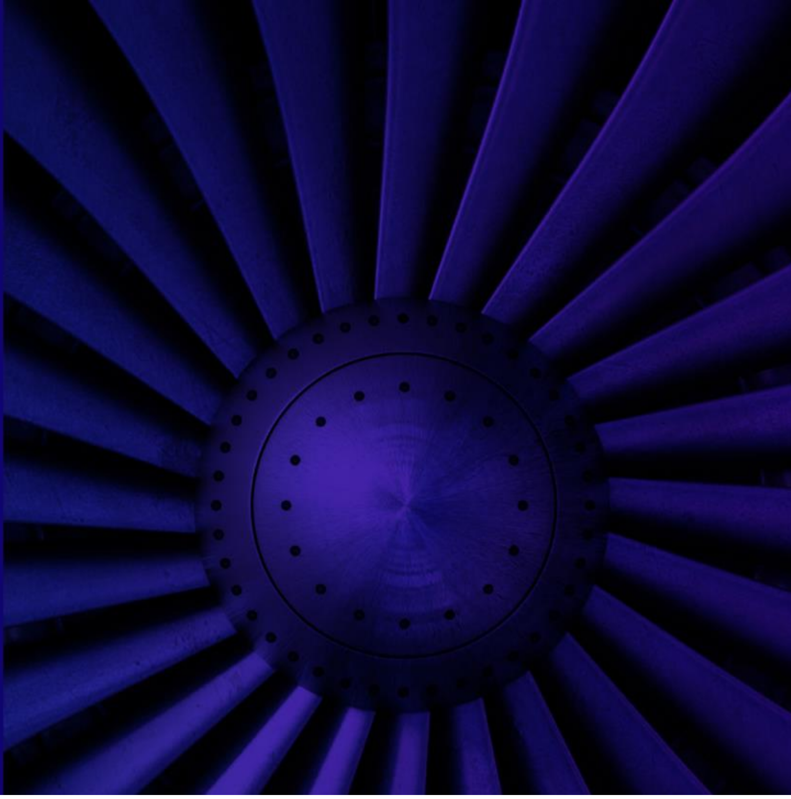
FIS

LexAlign

Security for Electronic Banking

Maximize security compliance monitoring and support for business customers.



Electronic Banking presents a unique set of risks as it has moved financial activities outside the security of the bank's walls to their remote business customers. Effective risk management requires the ability to identify security gaps and provide detailed guidance on how to remediate them, especially for treasury customers using products like RDC, ACH, and Wires. Weighing RISK without overburdening customers or your treasury staff is a challenge for many financial institutions.

Performing a security self-assessment is reasonably required by law or the customer's banking agreement. It is also a stated expectation in the regulatory guidance on RDC and ACH risk management.

"Specific contract provisions [should] include: Periodic audits of the RDC process, including the IT infrastructure[.]"

Source: FDIC FIL–4–2009, "Risk Management of Remote Deposit Capture," January 14, 2009

The solution from FIS' partner, LexAlign, automates the security assessment process and generates the records you and your customers need to demonstrate risk management. Your customers access the system when it's convenient for them and obtain essential, actionable guidance. And you get relevant information instantly via your secure, online dashboard.

BENEFITS of using LexAlign Security for Electronic Banking include:

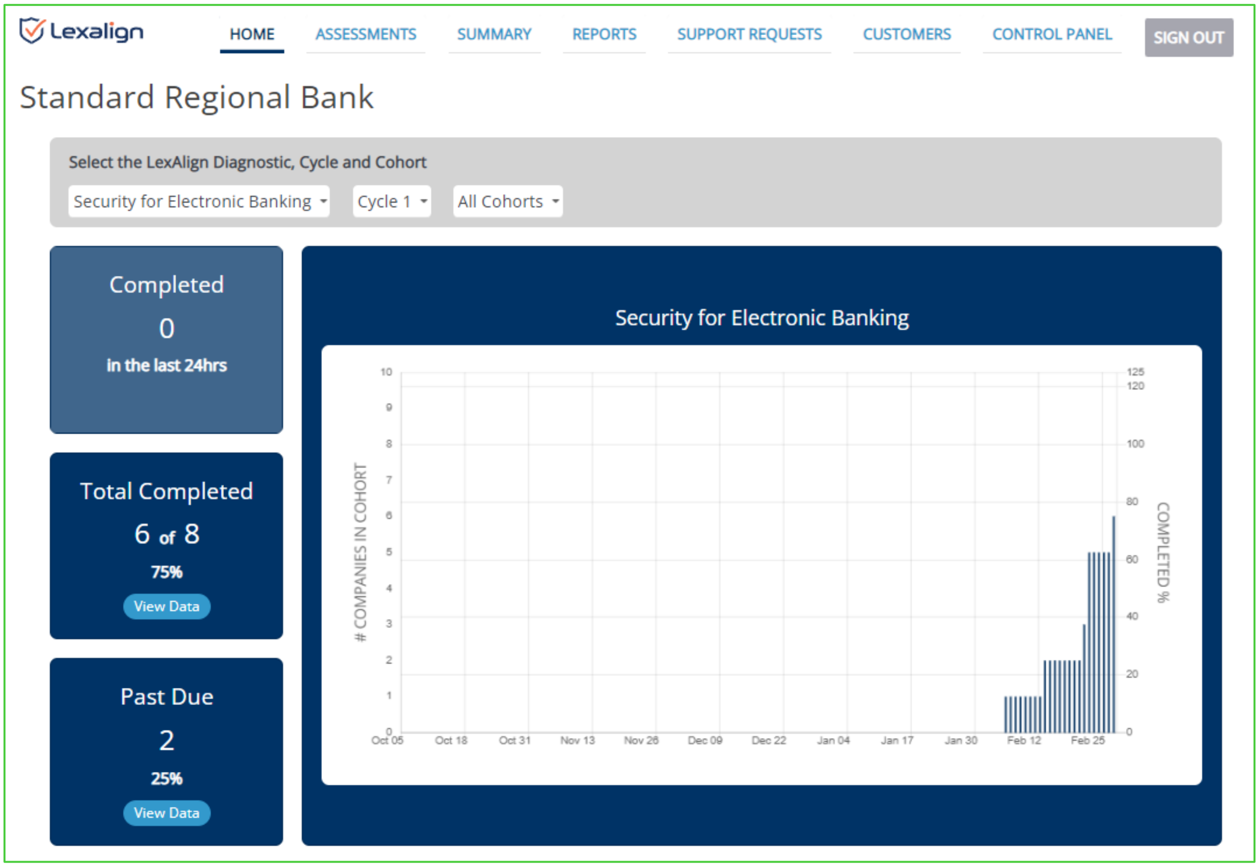
- Enables you to effortlessly show compliance with regulators' stated expectations on customer operational due diligence reasonably required for RDC, ACH and fraud risk management.
- Sensitizes customers to their risks and empowers them to remediate their gaps.
- Enables quantification and effective management of the staggering risks posed by remote customer operations, improving operational risk management and efficiency.

Key Product Features

- Comprehensive Financial Institution Dashboard that demonstrates risk management and enables easy data extraction for insight and actions.
- Focused Customer Dashboard.
- Intuitive, easy-to-use Self-Assessment for Customers.
- Actionable Insights for Customers, enabling *their* risk management at the frontline of fraud and loss.

Financial Institution Dashboard

The Home Page shows usage of LexAlign Diagnostics by Cycle and Cohort. This is your view of progress as a Cycle is executing through each Cohort.



Standard Regional Bank

Select the LexAlign Diagnostic, Cycle and Cohort

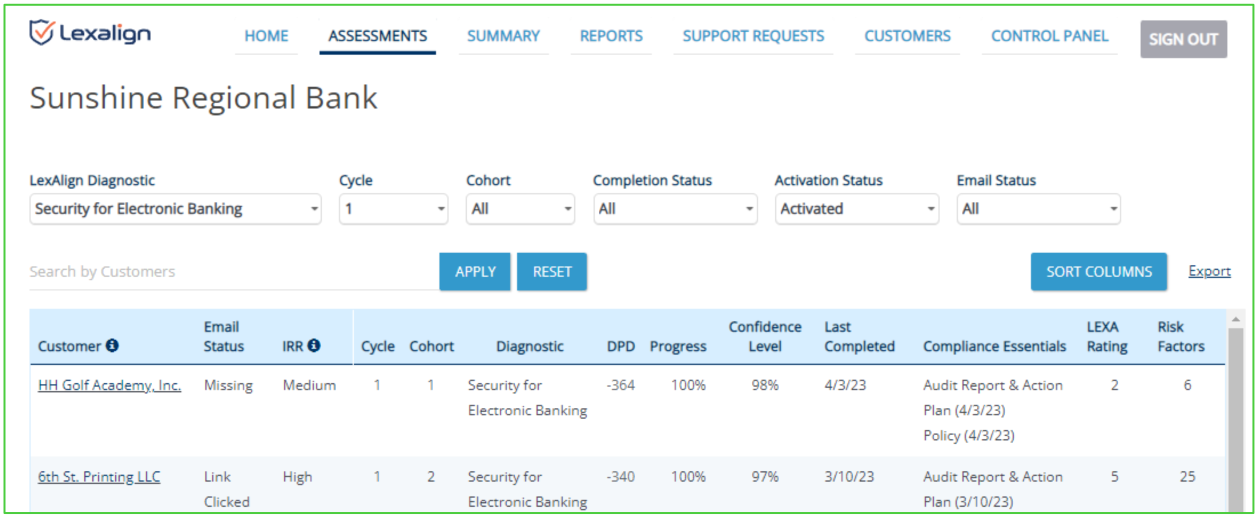
Security for Electronic Banking | Cycle 1 | All Cohorts

Completed
0
in the last 24hrs

Total Completed
6 of 8
75%
View Data

Past Due
2
25%
View Data

The Assessments Page replaces and improves upon the spreadsheets you've been using, especially for the burdensome task of tracking completion status. With LexAlign, it is all automated.



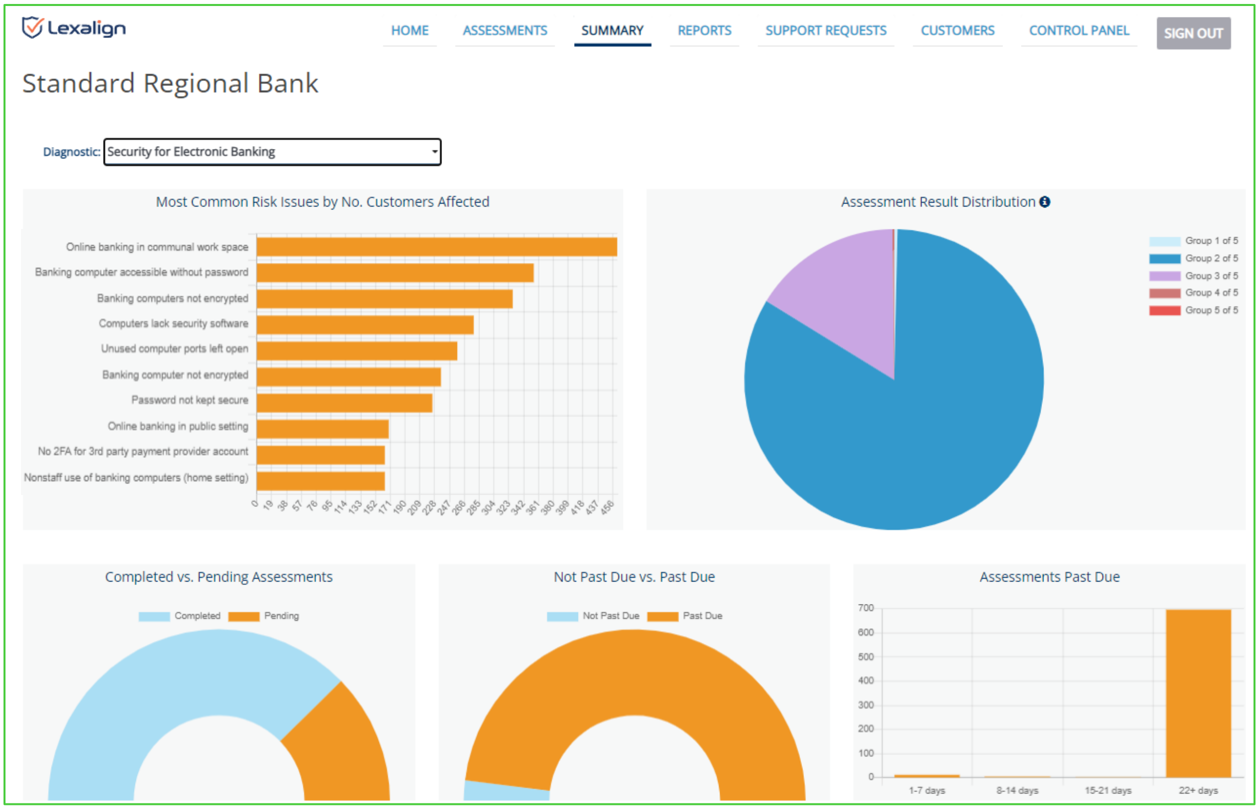
Sunshine Regional Bank

LexAlign Diagnostic: Security for Electronic Banking
Cycle: 1
Cohort: All
Completion Status: All
Activation Status: Activated
Email Status: All

Search by Customers

Customer	Email Status	IRR	Cycle	Cohort	Diagnostic	DPD	Progress	Confidence Level	Last Completed	Compliance Essentials	LEXA Rating	Risk Factors
HH Golf Academy, Inc.	Missing	Medium	1	1	Security for Electronic Banking	-364	100%	98%	4/3/23	Audit Report & Action Plan (4/3/23) Policy (4/3/23)	2	6
6th St. Printing LLC	Link Clicked	High	1	2	Security for Electronic Banking	-340	100%	97%	3/10/23	Audit Report & Action Plan (3/10/23)	5	25

The Summary Page demonstrates your Risk Management and Support. It can also help you prioritize remedial actions based on greatest potential impact. The information is presented by LexAlign Diagnostic.

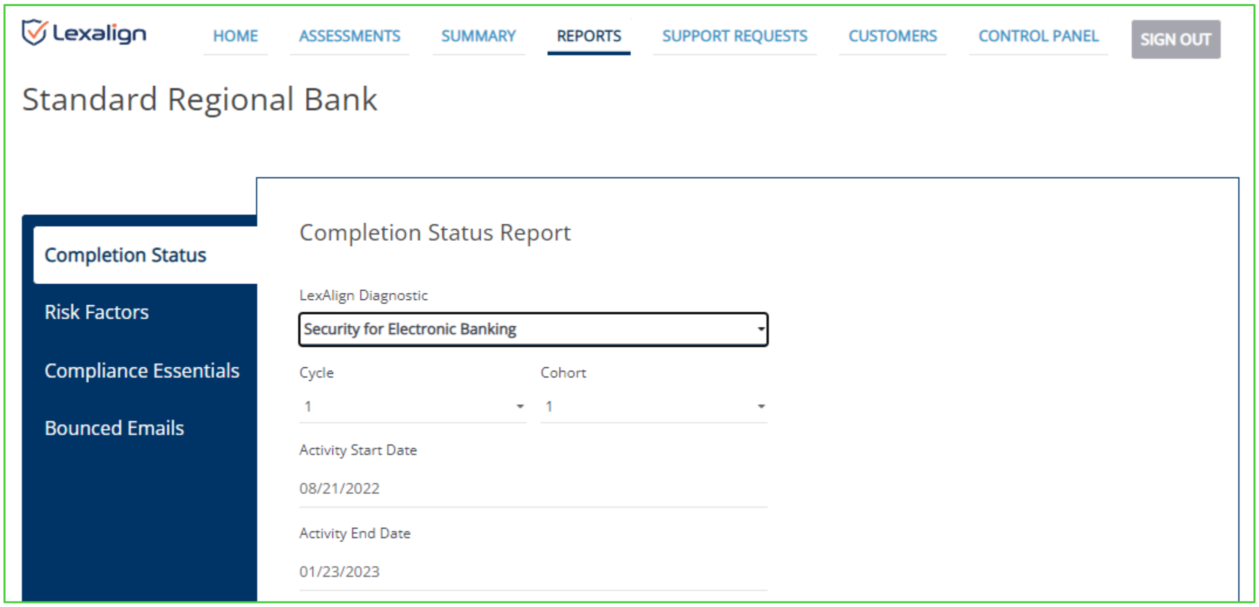

Lexalign
HOME
ASSESSMENTS
SUMMARY
REPORTS
SUPPORT REQUESTS
CUSTOMERS
CONTROL PANEL
SIGN OUT

Standard Regional Bank

Diagnostic: Security for Electronic Banking

Most Common Risk Issues by No. Customers Affected
Online banking in communal work space
Banking computer accessible without password
Banking computers not encrypted
Computers lack security software
Unused computer ports left open
Banking computer not encrypted
Password not kept secure
Online banking in public setting
No 2FA for 3rd party payment provider account
Nonstaff use of banking computers (home setting)
0 19 38 57 76 95 114 133 152 171 190 209 228 247 266 285 304 323 342 361 380 399 418 437 456
Assessment Result Distribution
Group 1 of 5
Group 2 of 5
Group 3 of 5
Group 4 of 5
Group 5 of 5
Completed vs. Pending Assessments
Completed
Pending
Not Past Due vs. Past Due
Not Past Due
Past Due
Assessments Past Due
700
600
500
400
300
200
100
0
1-7 days
8-14 days
15-21 days
22+ days

The Reports Page offers detailed reporting by Diagnostic for Completion Status, Risk Factors, Compliance Essentials, and Bounced Emails.



Standard Regional Bank

Completion Status Report

LexAlign Diagnostic: Security for Electronic Banking

Cycle: 1

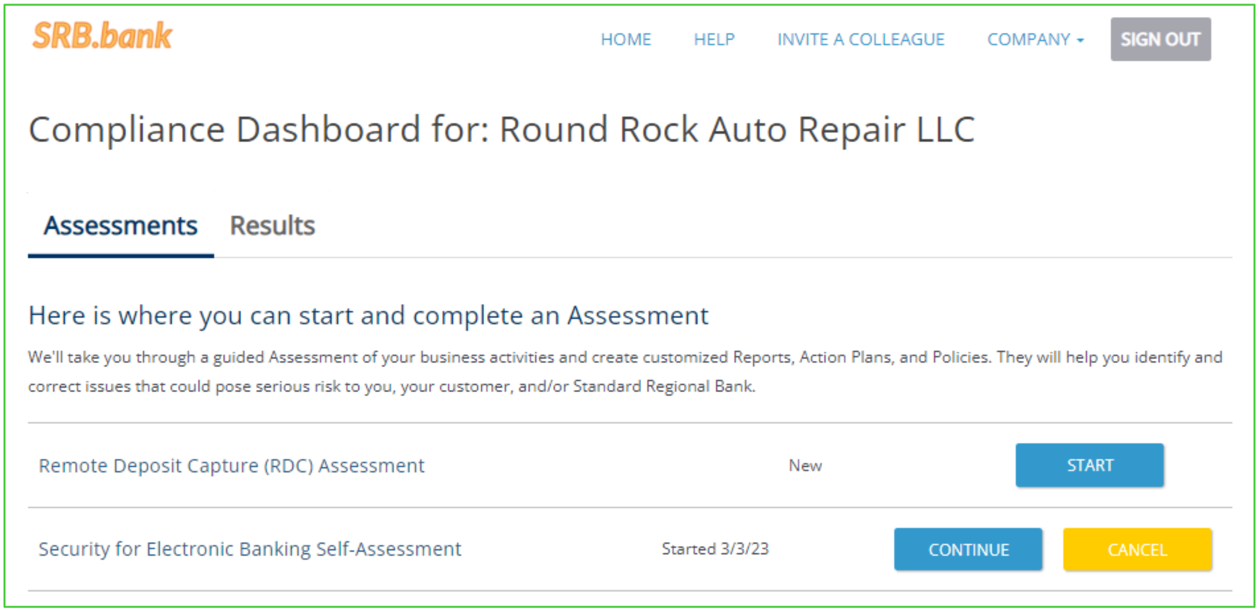
Cohort: 1

Activity Start Date: 08/21/2022

Activity End Date: 01/23/2023

Customer Dashboard

An easy-to-use starting point for your customers to begin or continue assessments.



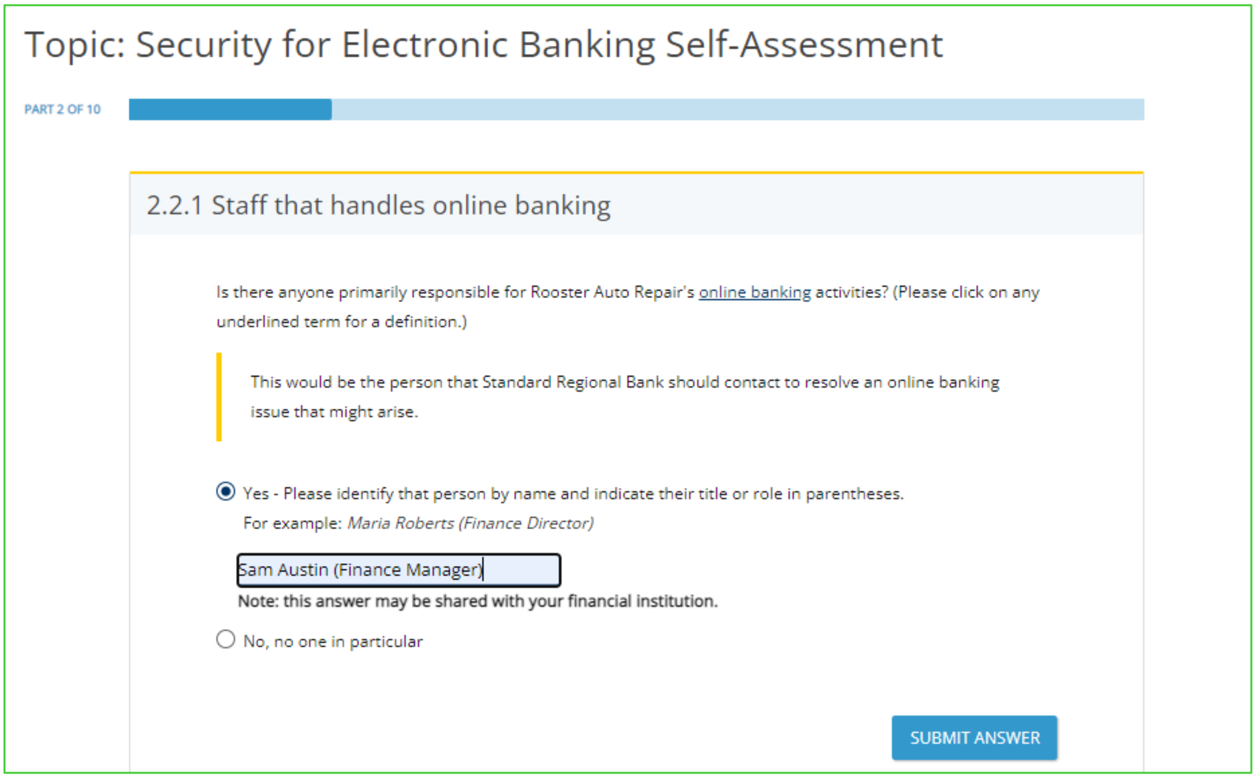
Compliance Dashboard for: Round Rock Auto Repair LLC

Here is where you can start and complete an Assessment

We'll take you through a guided Assessment of your business activities and create customized Reports, Action Plans, and Policies. They will help you identify and correct issues that could pose serious risk to you, your customer, and/or Standard Regional Bank.

Remote Deposit Capture (RDC) Assessment	New	START
Security for Electronic Banking Self-Assessment	Started 3/3/23	CONTINUE CANCEL

LexAlign Assessments are designed as diagnostic interviews that reflect regulatory requirements and stated expectations, and industry best practices.



Topic: Security for Electronic Banking Self-Assessment

2.2.1 Staff that handles online banking

Is there anyone primarily responsible for Rooster Auto Repair's online banking activities? (Please click on any underlined term for a definition.)

> This would be the person that Standard Regional Bank should contact to resolve an online banking issue that might arise.

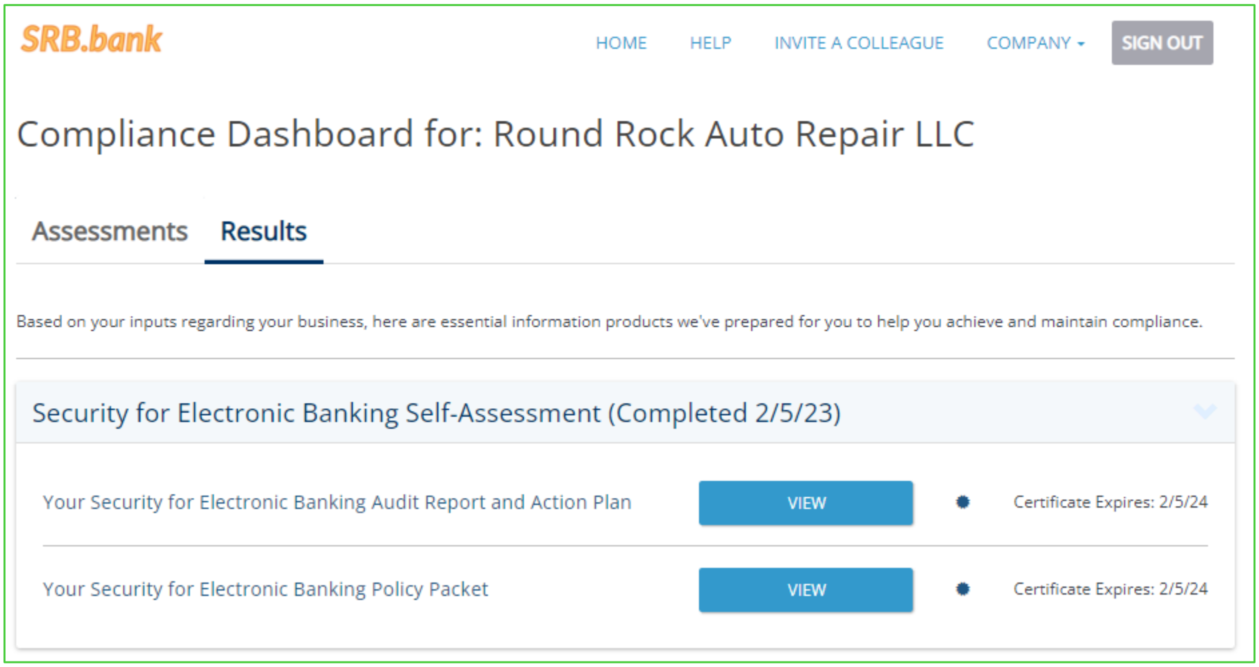
● Yes - Please identify that person by name and indicate their title or role in parentheses.
For example: *Maria Roberts (Finance Director)*

Sam Austin (Finance Manager)

Note: this answer may be shared with your financial institution.

○ No, no one in particular

Upon completing an Assessment, customers immediately get a detailed audit report, including a gap analysis and related action plan, and a policy package for training their staff.



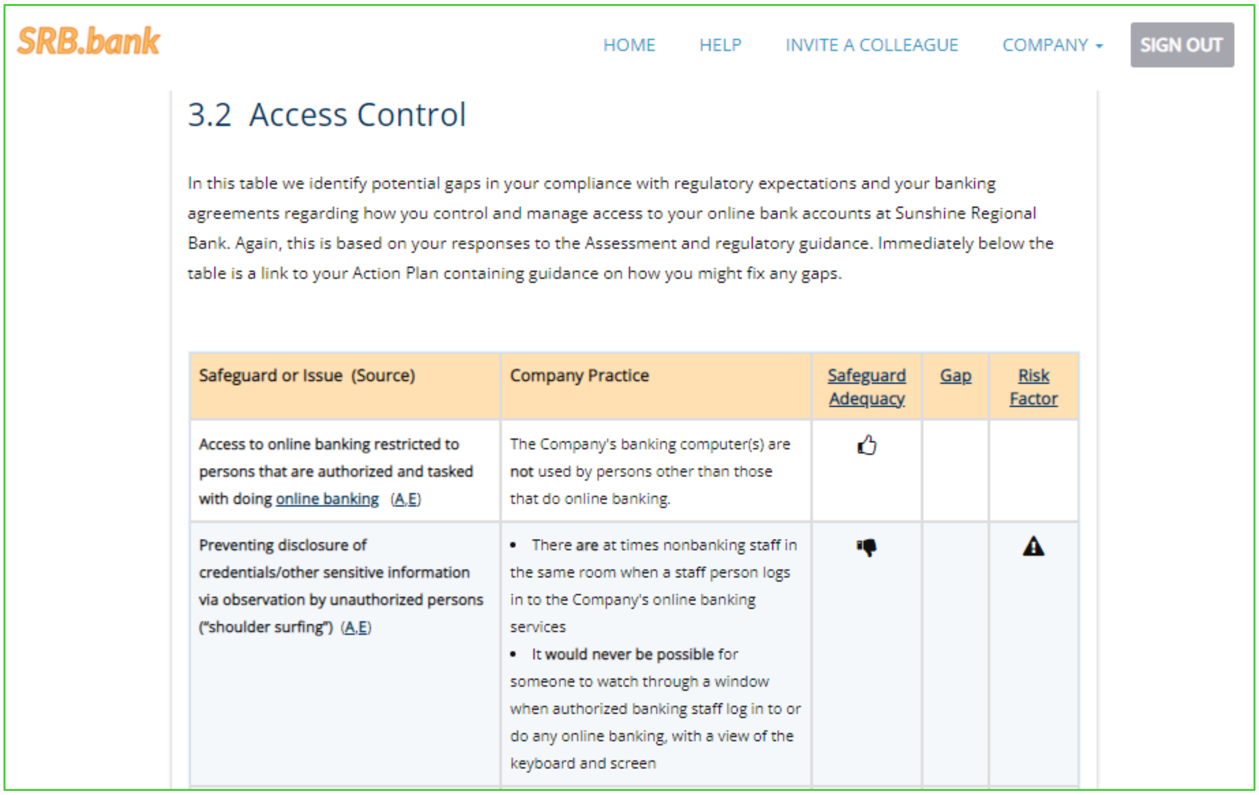
Compliance Dashboard for: Round Rock Auto Repair LLC

Based on your inputs regarding your business, here are essential information products we've prepared for you to help you achieve and maintain compliance.

Security for Electronic Banking Self-Assessment (Completed 2/5/23)

Your Security for Electronic Banking Audit Report and Action Plan	VIEW	Certificate Expires: 2/5/24
Your Security for Electronic Banking Policy Packet	VIEW	Certificate Expires: 2/5/24

The gap analysis compares company practices against regulatory requirements and expectations and industry best practices.

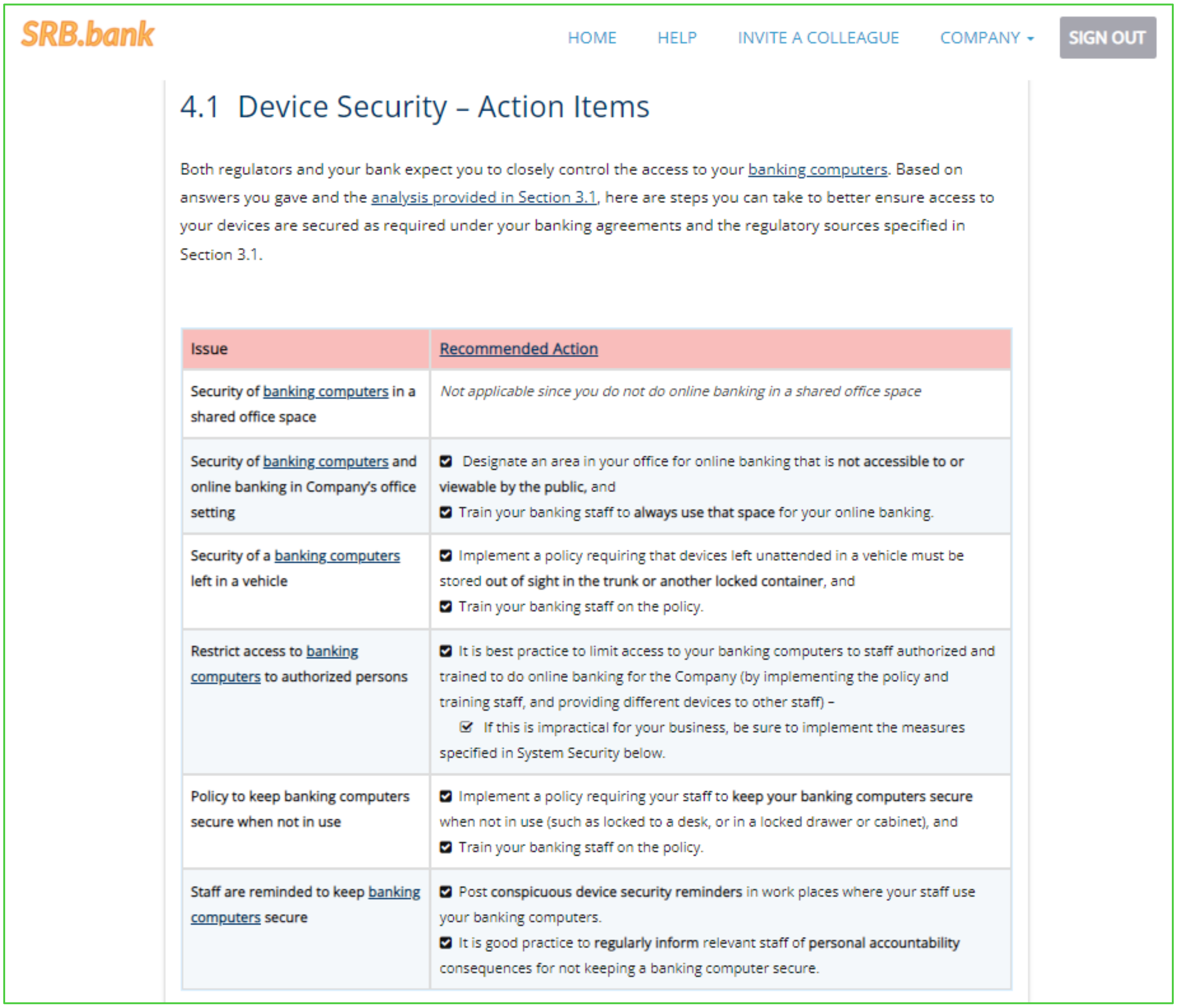


3.2 Access Control

In this table we identify potential gaps in your compliance with regulatory expectations and your banking agreements regarding how you control and manage access to your online bank accounts at Sunshine Regional Bank. Again, this is based on your responses to the Assessment and regulatory guidance. Immediately below the table is a link to your Action Plan containing guidance on how you might fix any gaps.

Safeguard or Issue (Source)	Company Practice	Safeguard Adequacy	Gap	Risk Factor
Access to online banking restricted to persons that are authorized and tasked with doing online banking (A,E)	The Company's banking computer(s) are not used by persons other than those that do online banking.	👍		
Preventing disclosure of credentials/other sensitive information via observation by unauthorized persons ("shoulder surfing") (A,E)	- There are at times nonbanking staff in the same room when a staff person logs in to the Company's online banking services - It would never be possible for someone to watch through a window when authorized banking staff log in to or do any online banking, with a view of the keyboard and screen	👎		⚠

The action plan contains clear instructions to remediate any issues uncovered.

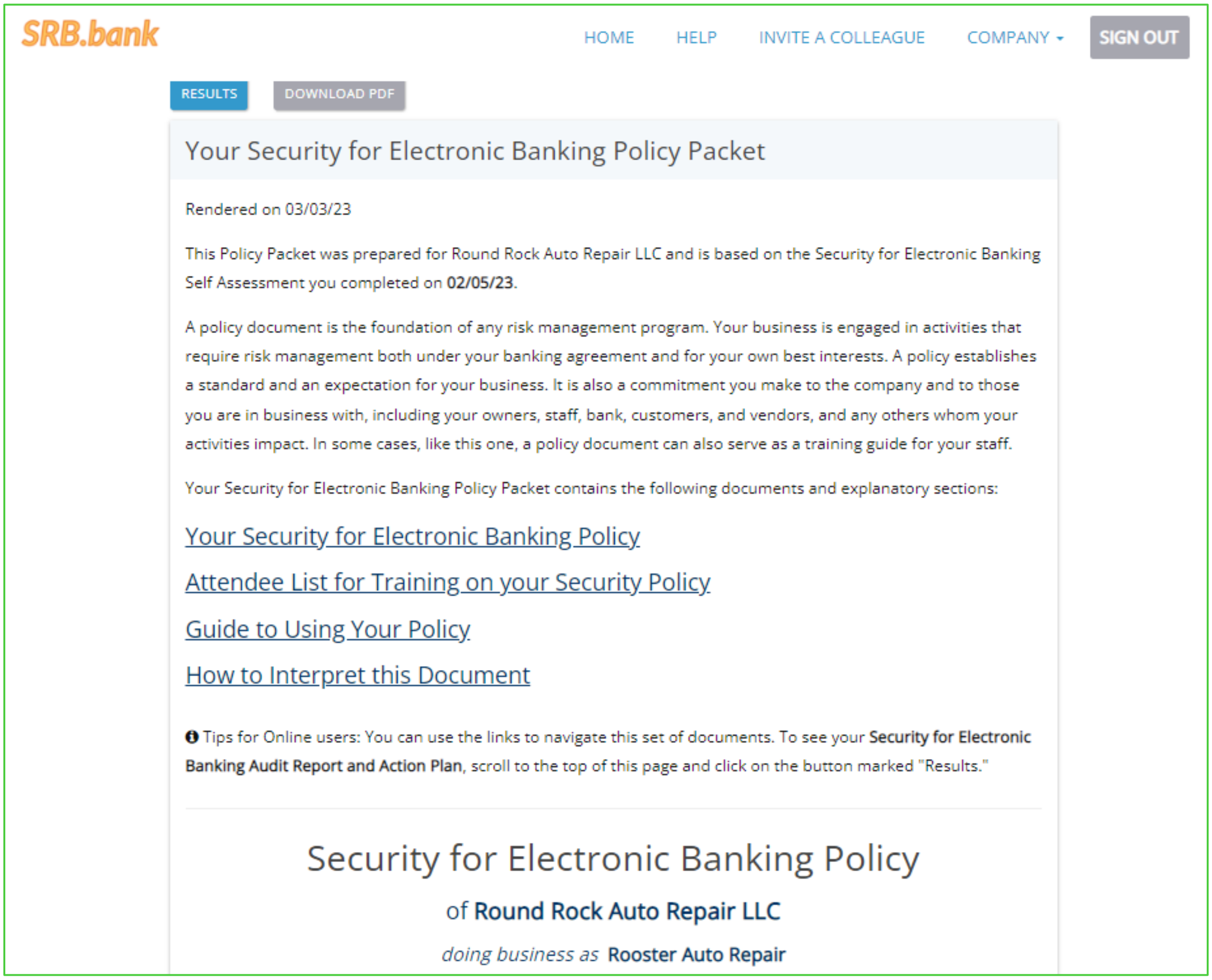


4.1 Device Security – Action Items

Both regulators and your bank expect you to closely control the access to your banking computers. Based on answers you gave and the analysis provided in Section 3.1, here are steps you can take to better ensure access to your devices are secured as required under your banking agreements and the regulatory sources specified in Section 3.1.

Issue	Recommended Action
Security of banking computers in a shared office space	*Not applicable since you do not do online banking in a shared office space*
Security of banking computers and online banking in Company's office setting	☑ Designate an area in your office for online banking that is **not accessible to or viewable by the public**, and ☑ Train your banking staff to **always use that space** for your online banking.
Security of a banking computers left in a vehicle	☑ Implement a policy requiring that devices left unattended in a vehicle must be stored **out of sight in the trunk or another locked container**, and ☑ Train your banking staff on the policy.
Restrict access to banking computers to authorized persons	☑ It is best practice to limit access to your banking computers to staff authorized and trained to do online banking for the Company (by implementing the policy and training staff, and providing different devices to other staff) – ☑ If this is impractical for your business, be sure to implement the measures specified in System Security below.
Policy to keep banking computers secure when not in use	☑ Implement a policy requiring your staff to **keep your banking computers secure** when not in use (such as locked to a desk, or in a locked drawer or cabinet), and ☑ Train your banking staff on the policy.
Staff are reminded to keep banking computers secure	☑ Post **conspicuous device security reminders** in work places where your staff use your banking computers. ☑ It is good practice to **regularly inform** relevant staff of **personal accountability** consequences for not keeping a banking computer secure.

An essential policy packet is provided that is designed for training their staff.



Your Security for Electronic Banking Policy Packet

Rendered on 03/03/23

This Policy Packet was prepared for Round Rock Auto Repair LLC and is based on the Security for Electronic Banking Self Assessment you completed on **02/05/23**.

A policy document is the foundation of any risk management program. Your business is engaged in activities that require risk management both under your banking agreement and for your own best interests. A policy establishes a standard and an expectation for your business. It is also a commitment you make to the company and to those you are in business with, including your owners, staff, bank, customers, and vendors, and any others whom your activities impact. In some cases, like this one, a policy document can also serve as a training guide for your staff.

Your Security for Electronic Banking Policy Packet contains the following documents and explanatory sections:

Your Security for Electronic Banking Policy

Attendee List for Training on your Security Policy

Guide to Using Your Policy

How to Interpret this Document

🛈 Tips for Online users: You can use the links to navigate this set of documents. To see your **Security for Electronic Banking Audit Report and Action Plan**, scroll to the top of this page and click on the button marked "Results."

Security for Electronic Banking Policy

of **Round Rock Auto Repair LLC**

doing business as **Rooster Auto Repair**

Contact Us

For more information, contact your FIS Account Executive or visit fisglobal.com.