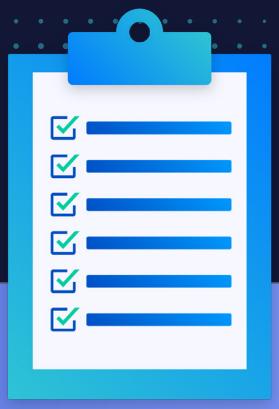
smarsh®

Scorecard

Hybrid Workforce Risk Assessment



Calculate your financial services organization's risk level as the workplace splinters between the office, remote or both

It wasn't that long ago businesses across the world were scrambling to enable remote work, quickly. Collaboration tools like Microsoft Teams, Zoom and Slack became crucial substitutes for conference rooms and desk pods, almost overnight. Now, with eyes on return-to-office plans, it seems we've entered yet another new realm: the hybrid work model.

For regulated financial firms, which are obligated to preserve and monitor communications, the shift from the office, to remote, to a hybrid of the two requires a major reexamination of business operations. This includes efforts devoted to risk mitigation, cybersecurity and the enablement of modern communications technology.

If you're reading this, you likely have some concerns about your organization's risk profile as the workplace dynamic continues to shift. You've come to the right place. **This DIY scorecard will help you identify and prioritize areas of information risk and determine a plan of action.**

*(**Directions:** Note your score for each Risk Factor in the far-right Score column. Add up your totals for each section to determine your current risk level.)*

Infrastructure

Let's start with your technology foundation. What kinds of changes did your company make to maintain business continuity and cybersecurity when employees went remote? What happens if/when they return to the office?

Risk Factor	Low-1	Medium-2	High-3	Score
Security controls (password policies, anti-virus, etc.)	Controls enabled & actively monitored across all locations	Security controls periodically audited	Security controls tested/ audited on demand	
Hardware & devices	Fully automated provisioning & updates in place	Use of approved and prohibited devices outlined by policies	Use of unapproved devices or hardware not defined.	
Network & WiFi	Network access protocols defined and regularly audited	Network access protocols defined and audited as needed	Network access protocols not defined or audited	

Infrastructure score _____

Policies and procedures

A robust risk assessment will require some deep organizational introspection. Make sure to include all relevant stakeholders to reevaluate your compliance processes (compliance), your internal communications policies (legal), and how you choose technology vendors (IT).

Risk Factor	Low-1	Medium-2	High-3	Score
New tool evaluation	Ongoing, cross-functional process	On-demand, led by technology & business	Ad hoc, or process not defined	
New feature evaluation	Ongoing, cross-functional process	On-demand, led by technology & business	Ad hoc, or process not defined	
Retention policies	Updated reflecting all accepted channels	General policies reflecting all channels uniformly	Defined only for user defined business records	
Code of conduct	Updated reflecting all accepted channels	General policies reflecting all infractions uniformly	General policies primarily focused on in-person infractions	
Supervisory policies	Regularly updated policies reflecting acceptable use policies	General policies updated on ad hoc or as needed basis	General policies not regularly updated	
Supervisory review	Review audited as effective for remote and in-person staff	Remote review process defined on case-by-case basis	Review process not currently defined or updated	
Conduct surveillance	Automated inspection of all business communications	Inspection managed with tools depending on investigation	On-demand, manual inspection against infractions	
Prohibited networks	Automated inspection for use of prohibited networks	On-demand inspection for use of prohibited networks	No policy defined to investigate prohibited networks	

Policies and procedures score _____

Employee training

It only takes one email, text message, or social media post to compromise security or compliance. To protect your organization from cybersecurity, regulatory or legal issues, employee training for digital communications is essential. Train employees on potential information risks and how to avoid them. Trainings should be held often, accessible to all staff and updated to reflect company changes.

Risk Factor	Low-1	Medium-2	High-3	Score
Tool usage	Training specific to use of tools by specific functions	General training provided for select function	Training provided ad hoc and on-demand	
Prohibition policies	Consequences for policy violations clearly defined	Prohibited policy training defined within general training	Prohibited networks not addressed within training programs	

Risk Factor	Low-1	Medium-2	High-3	Score
Compliance	Employee tested & certified on applicable record keeping & supervisory obligations	Employee training on compliance requirements provided on-demand	No formal user training for compliance requirements	
Security & privacy	Employee tested & certified on applicable security & privacy obligations	Employee training on security & privacy requirements provided on-demand	No formal user training for security & privacy requirements	
Employee attestation	Ongoing, regulatory audited attestation programs in place	Sometimes require attestation	No formal attestation program in place	

Employee training score _____

Communications controls

Do you know which channels employees are using to communicate? Have those platforms or tools been properly vetted? Are they using personal accounts? (If you're unsure, you may need to go back and adjust your score accordingly.) As you go through each channel, consider the benefits of a cloud-based, end-to-end compliance solution — especially as new communications tools are introduced.

Risk Factor	Low-1	Medium-2	High-3	Score
Public social media (Twitter, LinkedIn, Facebook, etc.)	Automated capture and archive for accepted channels	Semi-automated capture and archive for select users	Channel used but not captured or archived	
Messaging apps (WeChat, TikTok, WhatsApp, Jabber)	Automated capture and archive for accepted channels	Semi-automated capture and archive for select users	Channel used but not captured or archived	
Mobile device content (text and other BYOD and corp device content)	Automated capture and archive for accepted channels	Semi-automated capture and archive for select users	Channel used but not captured or archived	
Collaboration (Microsoft Teams, Slack)	Automated capture and archive for accepted channels	Semi-automated capture and archive for select users	Channel used but not captured or archived	
Email (Office365, Gmail, Bloomberg)	Automated capture and archive for accepted channels	Semi-automated capture and archive for select users	Channel used but not captured or archived	
Video conferencing (Zoom, WebEx, RingCentral)	Automated capture and archive for accepted channels	Semi-automated capture and archive for select users	Channel used but not captured or archived	

Communications controls score _____

Your Results:

Total score _____

0-22 Points: Risk? What risk?

Well done. You have made information risk a priority. Alas, regulatory compliance, data privacy requirements, and other legal risks don't leave much room for gray area. Even the slightest infraction can jeopardize your growth. Let us help you tie up any loose ends.

23-44 Points: Getting riskier...

You've got some adjustments to make to your risk mitigation plan, but now you know where your strengths and weaknesses lie. With expert guidance, you can improve that score and stay on track.

45-66 Points: RISK ALERT!

Your risk mitigation strategy (or lack thereof) could be costing you. Time to call the experts at Smarsh.

Our experts are waiting to help you.
Contact us to schedule a risk assessment follow up chat.

Smarsh has worked with financial services organizations of all sizes for over 20 years. In that time, communications preferences and work models have drastically changed and the regulatory landscape has evolved. To meet every moment, Smarsh has made ongoing innovations to help clients manage compliance, mitigate risk and stay competitive.

smarsh®