How to Delegate Responsibilities to Reduce Compliance Risk



Opinions expressed by Entrepreneur contributors are their own.

Compliance leaders like chief information security officers are faced with the ever-growing responsibility of minimizing the risks their companies face. However, it’s not reasonable for them and their teams alone to be accountable for lowering risk. Compliance needs to be a duty that belongs — at least in part — to all members of the organization.

This doesn’t mean passing the proverbial buck. If you’re the head of risk and compliance, you’re the one who will answer for any issues that arise. Still, you can’t be expected to do it all. That’s a recipe for health disasters. After all, 90% of CISOs say they regularly deal with at least moderate

stress, online service company Nominet reported.

To lower your chance of professional burnout, begin to delegate to others both in and out of your vertical. Feel uneasy at the prospect? There are several steps you can take to delegate responsibly and securely. That way, no one will be able to sabotage your company's compliance efforts, and you'll have fewer tasks to accomplish.

Related: 7 Rules for Entrepreneurs to Delegate Effectively

1. Map out your delegation strategy first

Rather than just delegating duties piecemeal, construct a delegation chart. Include what you intend to delegate, who it will be delegated to, and how it will be monitored.

For instance, security training is essential but can be time-consuming if your organization deals with sensitive information. Delegating this responsibility to a designated security employee can help alleviate the burden. Ensure that the employee is adequately trained and that their performance is monitored regularly to maintain compliance with security protocols. By delegating this responsibility, you assign ownership and authority within specific parameters while maintaining overall control.

Once you have created your chart for particular tasks, you can feel more comfortable delegating responsibilities. Just be sure to make the chart transparent to everyone on it so people know where ownership lies.

2. Put a premium on

operationalizing security tasks (or tools that accomplish it for you)

It can feel uncomfortable to transfer tasks, particularly those that relate to compliance and security. By operationalizing security practices into standard operational processes, such as onboarding and offboarding new employees and tech stack applications, you can safeguard against those tasks that might otherwise fall through the cracks and enable your employee base to contribute to the broader risk management strategy.

As noted by CPO Magazine, 88% of security problems are related to human error. Adding secondary “just in case” checkups to important tasks helps identify existing errors quickly. Risk management tools should be included in your strategy to scan for and alert you to anomalies and areas of risk. Finding anomalies leads to quick alerts and opportunities for you to respond quickly.

Verifying all your delegation workflows as a matter of course may prove advantageous if you’re audited, too. As noted by Kevin Brown, Information Security Officer at risk management platform Ostendio:

“Security is about more than complying with a framework. Organizations should focus their efforts on data security and risk management planning first, and with the right discipline, they can develop the policies and procedures necessary to pass complex security audits.”

You can consider implementing a tool that allows you to cross-walk across multiple security frameworks and track the implications of operational activity on security as one of those protective procedures.

3. Generate tracking methods for all delegated assignments

If you aren’t already using a project management software tool, consider adding one for all delegated security-related assignments. You want to have a track record that’s visible to every task’s stakeholders. This reduces the risks and threats related to potential errors or missed steps.

Related: 5 Project Management Systems to Streamline Your Business Processes

Ideally, the project management module or tool should make it easy to get a snapshot of what’s happening across your security landscape. At any moment, you should be able to log on and see if security, compliance and risk management tasks are up-to-date.

In case of a problem, you’ll be glad you have a way to discover gaps and loopholes. It’s always better if you find places of concern before they cause major headaches. Tracking all communications, actions, and owners in a single source of truth makes you more efficient.

4. Conduct risk assessments before delegating to outsourced third parties

Plenty of third-party entities tout their abilities to keep your company compliant with security frameworks. And outsourcing some aspects of your risk management can be a smart way to delegate. The problem? You can’t control what third parties do.

Conducting a comprehensive investigation to make sure that they’re able to live up to their promises is your best bet.

After choosing a third-party vendor you feel will serve your needs, conduct a third-party risk assessment to ensure they protect your organization from a potential breach.

Since risk is everyone's job at your organization, be sure other departments are equally as cautious. You need to know the ways they evaluate third-party providers. The last thing you want is for someone to expose your company's data by contracting through the wrong third party.

5. Explain the reason behind regulation when delegating.

To cover all your bases when delegating outside of your department, take a teaching approach. Rather than just telling others what to do, give them the reasoning behind why they're doing it. As you know, regulations and laws can be very confusing, even to knowledgeable people. Spending time in "educator mode" stresses the importance of the task you're delegating.

Being informative serves an extra purpose as well. The more other employees (and not just your direct reports) understand compliance and risk management, the better. It's much easier to get everyone on board with security practices and procedures if they're aware of why they matter.

Remember: Avoiding risks whenever possible is something everyone can do. Yes, it's your job description to head up compliance and security. But you can't make decisions for all your colleagues. Sharing key information allows anyone to make informed choices built on facts.

You may feel like you can't possibly pass along many of your responsibilities. But if you don't, you'll limit your ability to perform high-level functions. So go ahead and delegate tasks. Just make sure you've set up structured governance to

keep everything securely on track.

https://www.entrepreneur.com/science-technology/reducing-compliance-risk-a-guide-to-delegating/450560