Regular Risk Assessments Are Crucial to Compliance

Merely telling a compliance regulator that you have implemented cybersecurity measures without knowing the risks to your business is not going to cut it. Data protection regulations worldwide also hold you accountable to undertake risk assessments regularly and document both the results and your remediation efforts.

A risk assessment is truly the best place to start in your journey to achieve and maintain compliance. How can you possibly know what your most critical security risks and vulnerabilities are without a thorough and accurate examination of where you stand right now?

Risk assessments are more than just filling a checklist and must become a part of your business' standard operating procedures.

IN FACT

conducting risk assessments is part of the core security measures mandated for many well-known regulations such as GDPR, HIPAA, PIPEDA, ISO 27001, FISMA and the list goes on. Failure to do so could lead to a host of punitive actions that disrupt and even damage your business.

Risk Assessment: More Than Just a Checklist

Executing a risk assessment goes beyond checklists and questionnaires. Ticking boxes off or simply answering questions will not satisfy regulatory mandates, as your word is practically worthless without a thorough examination and results that have been verified and proven as accurate.

Additionally, merely carrying out surface-level assessments will not suffice. A risk assessment is a comprehensive process wherein you peel back the layers to analyze and identify risks in your network and throughout your supply chain. This will truly help you ward off cyberthreats and convince a regulator or your cyber insurance provider about your commitment to data protection.

Treat every assessment as an under-the-skin scan of your entire IT environment by providing answers to questions like these:

What data and information assets are stored?

How is the data collected, processed or managed?

Are the network and all your devices properly encrypted and secured?

Are the systems and hardware regularly updated with security patches and protected with antivirus/antimalware software?

What users have access to the network and the data?

How is user access managed and are identities securely verified?

What are the most common security risks your business and supply chain are vulnerable to?

What user credentials from your network have already been exposed or stand to be exposed on the Dark Web?

Positive ROI and Peace of Mind

Implementing an ongoing risk assessment strategy can fetch you positive ROI and peace of mind:

DEMONSTRATE COMPLIANCE AND DUE CARE

Documented proof that you recently completed risk assessments is a required component of a regulatory audit, whether conducted at random or when triggered by a security incident such as a criminal theft, data breach, or other cyberattack. It is also a critical element to validating due care efforts when filing a cyber insurance claim.

PROACTIVELY AVOID CYBERTHREATS

Being aware of all possible security vulnerabilities in your network and throughout your supply chain helps you significantly reduce the likelihood of potentially malicious threats successfully disrupting or harming your business.

REDUCE LONG-TERM COSTS

It goes without saying that you could potentially prevent reductions in revenue due to lost sales and/or reputational damage by identifying security risks and working towards tackling them before they turn into bigger problems.

DISCOVER CRUCIAL INSIGHTS

By regularly analyzing your risks status, you stand to gain a record of crucial insights on matters such as frequently recurring security gaps and risks, anomalous activities or network changes, and the security controls and procedures you must manage to keep up with the growth of your business and the cyberthreats.

GAIN COMPETITIVE ADVANTAGE

Your brand reputation grows further only when prospects and clients are assured you are doing your best to keep their data safe.

Make Ongoing Assessments a Standard Operating Procedure

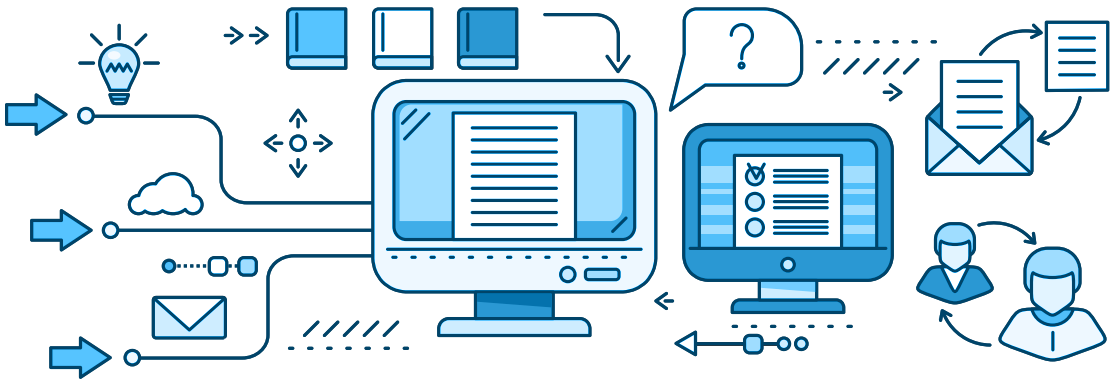
In a world of rapidly evolving technology and cyberthreats, a single random risk assessment is only a point in time measurement, as the results and risks will continue to change and evolve.

Add to your standard operating procedure a strategy to conduct risk assessments regularly, document all remediation efforts and leverage all the insights and risk analysis to optimize your security and compliance efforts.

Simplify the Compliance Process

Compliance is complicated and often a huge challenge to tackle on your own. It takes a special set of skills and tools to perform a thorough and accurate risk assessment, which includes delving deep into the inner workings of your network and infrastructure.

We specialize in helping businesses like yours successfully execute the required risk assessments to achieve compliance. We provide comprehensive reporting and clear remediation plans to address any risks or gaps you uncover, as well as the technical support you need to help simplify the risk management process.



Schedule a compliance risk assessment today to proactively identify and resolve any security risks in your business before they lead to bigger problems.

J & M Security Solutions
888-819-3045
info@jandmsecuritysolutions.com
www.jandmsecuritysolutions.com