

Raising the bar on cybersecurity

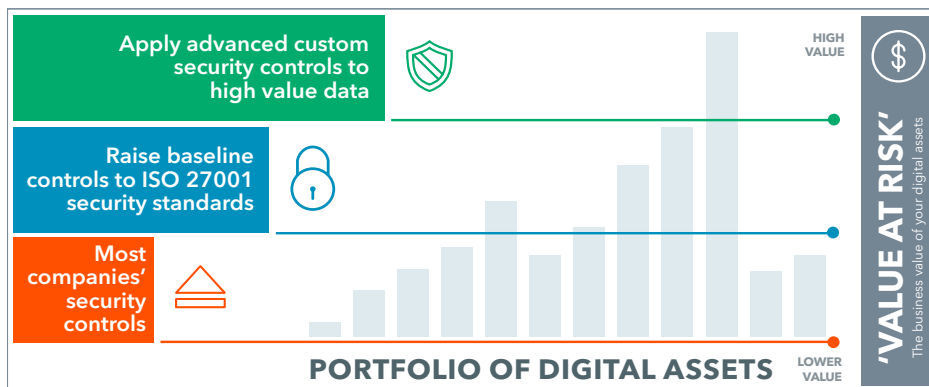
DOES YOUR LAW PRACTICE HAVE A COMPREHENSIVE INFORMATION RISK MANAGEMENT PROGRAM?

According to the latest data from the American Bar Association, 80 percent of the top 100 largest law firms in the United States have experienced data breaches. Information security experts now agree that law firms represent the next fertile frontier for hackers. Why? Because law firms store valuable data about their clients, but seldom have sufficient information risk management programs in place to safeguard this data.

Cyber attacks pose the greatest threat to the confidentiality and trust inherent in the attorney-client relationship. Legal firms have an ethical obligation to ensure that technologies and procedures used in client representation do not subject confidential information to unauthorized disclosure. Today, clients are asking their legal firms to provide assurance that they have the right security measures in place to keep their information safe. It should be the ethical obligation of every lawyer and law firm to provide that security.

As information risk management becomes a top priority for law firms, managing partners and members struggle with where to focus their information security time and money.

Focus security dollars on assets that represent the greatest risk



Achieving comprehensive cyber risk management

Aprio empowers managing partners and members to recognize the right things that should be happening within their organizations and with vendors to effectively mitigate information risks and instill client trust. We help legal firms grow with confidence through our comprehensive information risk management methodology.

- 1. Risk analysis.** We begin with a thorough understanding of your firm's "digital assets" - critical groupings of data and processes that could harm the firm if compromised. Working side by side with your technical leaders, we uncover the most significant risks to these valuable information assets.
- 2. Gap assessment.** Next, we determine whether current risk management activities are appropriate given your firm's risk appetite and tolerance. We measure your activities against relevant aspects of leading security standards, such as ISO 27001.
- 3. Risk management.** By focusing on the value at risk, we enable you to maintain baseline information security controls that protect the majority of data and systems while selectively investing in advanced security measures to protect higher-value digital assets.
- 4. Ongoing monitoring and attestation.** After establishing this thorough understanding of your digital assets' relative value and risks, we deliver independent and objective attestation reporting to provide an added level of assurance that controls are operating effectively.

Today, clients are asking their legal firms to provide assurance that they have the right security measures in place to keep their information safe.

Raise the bar

A common misconception is that cybersecurity is a technical problem that can be addressed through vulnerability scans. However, these surface-level reports may fail to address the most significant risks to your firm. As a result, you could be throwing your money away on technical security measures that protect the wrong things.

Aprio looks deeper to assess your firm's entire information security management system - people, processes and technology. The net result delivers an ongoing risk management program that protects the integrity of the firm and keeps you ahead of the ever-changing threat environment.

A higher level of assurance

Our auditors and information assurance specialists provide independent attestation and certification against such frameworks as SOC 2, the PCI Data Security Standard and ISO 27001.

An attestation is a particularly rigorous type of assurance engagement in which an independent CPA expresses an opinion on a set of assertions. CPAs must comply with strict AICPA attestation standards, and they bear professional liability for their opinions.

So when Aprio attests to your information systems and controls, we have personal and professional "skin" in the game. No other type of information security report provides this level of assurance.

ISO 27001 certification

Aprio has been accredited as an ISO 27001 Certifying Body, making it the first full-service CPA firm to earn this credential.

An internationally accepted framework, ISO 27001 certification verifies that an organization has deployed a strong information security management system.

Most security breaches – 95 percent or more – could have been prevented by following ISO 27001 security management standards.



About Aprio

Since 1952, clients throughout the U.S. and across more than 40 countries have trusted Aprio for guidance on how to achieve what's next. As a premier, CPA-led professional services firm, Aprio delivers advisory, assurance, tax and private client services to build value, drive growth, manage risk and protect wealth. With proven expertise and genuine care, Aprio serves individuals and businesses, from promising startups to market leaders alike.

Aprio.com



Let us help you
raise the bar on
cybersecurity.
Contact:



Dan Schroeder
Partner-in-Charge,
Information Assurance Services
dan.schroeder@aprio.com
[770.353.8379](tel:770.353.8379)



Howard Zandman
Partner,
Litigation Support and Forensic
Accounting Services
howard.zandman@aprio.com
[404.814.4915](tel:404.814.4915)