

Ostendio



The MyVCM™ How-To Guide to Compliance

How does MyVCM help with my compliance assessment?

MyVCM is a platform designed to help organizations build, manage and maintain their information security and compliance program.

The first step we recommend any organization to take is to conduct an assessment to determine how your information security and compliance program rates today. Are you operating in a compliant mode? Where are the gaps? Which areas need to be strengthened?

To get started we recommend you take our online High Level Assessment. This confidential assessment takes just a few minutes to complete and you will immediately receive your organizations “Compliance Score”. This is intended to provide an initial guide to gaps in your information security and compliance program. It is a starting point and not intended to be a replacement for a broader enterprise wide risk assessment as defined in published guidelines such as ISO 27001, NIST 800-30 or the HIPAA Security Rule.

How does MyVCM help with my audit requirements?

Once a company signs on to MyVCM, we handhold you through the entire process of establishing your security and compliance program.

The first step is to conduct a High Level Control Audit. The Audit covers 3 key areas:

- What do you do today? We call this Stated Compliance - what procedures and processes do you have in place today?
- What do you have documented that you do? We call this documented compliance.
- What can you prove you have done? We call this evidence of compliance.

The High Level Control Audit (HCLA) is a simple, easy way to get a snap shot of your information security framework. MyVCM's HCLA is a proprietary process that is a simplified version of the ISO2700 and OCR audit protocols.

Completion of the HCLA provides a road map for what you need to do to set up an information security and compliance program. This will ensure you are best prepared for an audit.

How does MyVCM help with ongoing compliance reporting and management?

The ongoing management of your organizations compliance program is critical to the security of your organization. At the core of MYVCM is a SaaS based workflow management solution for ongoing compliance management. MyVCM gives you the ability to demonstrate your information security and compliance program to key stakeholders. This includes customers, partners, employees and vendors.

MyVCM provides a broad range of tools including an Executive Dashboard and Management reports to enable you to share key performance data. And as the information is online, MyVCM gives you the ability to share this real time with other organizations on the MYVCM Trust Network. So if your client is on the MyVCM Trust Network and wants to see how you manage compliance, you can easily demonstrate your program.

Does using MyVCM eliminate the need for costly third-party audits?

There are a number of reasons an audit may be required:

- A potential client may require you to do an independent security assessment before they bring you on as a vendor.
- Standards such as ISO 2700 have a requirement for an annual audit
- If you have a security breach you may have to answer to someone such as the Federal Government.

- Some pro-active audits are now being required by federal and state authorities
- An investor may require an audit when conducting due diligence.

However, by implementing and actively using MyVCM as part of a comprehensive information security and compliance program, the audit process will be simplified as you will be better prepared for the audit and more likely to pass it.

What do I have to do to prepare for my first MyVCM compliance effort?

We provide a turnkey solution and support services to help our clients get started on MyVCM and incorporate it into their daily operations. Between our platform and support staff we:

- Help you gather your organizational information and conduct a MyVCM High Level Control Audit
- Work with you to review results and determine gaps
- Help you create or collect your information security policies, training programs, audits and assets
- Evaluate progress by conducting a follow-up MyVCM High Level Control Audit
- Teach you how to manage your automated MyVCM workflows

How long will it take my firm to complete the first MyVCM compliance effort?

We always advise our clients that compliance is not a destination – something you done once and are done - it is a journey. A good program requires effort to not only build it but to manage and maintain it on an ongoing basis.

MyVCM provides a solution to help you build, manage and maintain your compliance program.

Who needs to be involved in setting up the MyVCM program?

The best information security and compliance programs involve everyone in the organization. This creates a culture of compliance. Certain regulations such as HIPAA require a named individual be responsible for information security.

Industry best practices recommend that a company have a Chief Security Offices and a Chief Privacy Offices. In many cases it may be the same individual. What is important is that not only is someone in charge of the physical aspects of security, but someone is also paying attention to and charged with protecting private and sensitive information.

How much effort is required to maintain MyVCM once the initial implementation is done?

The most important part of any program is to ensure it is properly maintained. MyVCM simplifies that process and reduces the effort required by automating all workflows.

When my firm is finished implementing our compliance program, can we market the fact that we're HIPAA and HITECH compliant?

There is actually no certification authority that determines HIPAA compliance. The reality is the best that organizations can do is to operate in a manner that is consistent with the regulatory framework. As a practical example OCR, the Government's Office for Civil Rights, reserves the right to make a judgment after the fact. They are looking to ensure organizations are doing what is reasonable under the guidelines.

Does MyVCM help with HITRUST certification?

HITRUST is a not-for-profit organization that established practices and standards. They will conduct a HITRUST audit. There is debate on whether

HITRUST is the best benchmark for smaller organization, as the bar is very high.

However if HITRUST is the standard you are adopting, MyVCM will help you build, manage and demonstrate your compliance.

What does a typical MyVCM engagement cost?

MyVCM is a platform-based solution with a low monthly fee for service. The pricing is structured on a fee-per-user basis. This provides your organization with an affordable and predictable cost and avoids expensive and often unpredictable charges for professional service engagement.

If you have any additional questions or need help developing or improving your compliance program, please contact us at info@ostendio.com.