HITRUST®

and the cloud

What you should know about using cloud platforms

By Jason Papador, consultant at Wipfli

When it comes to the cloud, do you meet HITRUST CSF requirements?

The HITRUST CSF® is one of the most widely adopted security and privacy frameworks. As a HITRUST Authorized External Assessor, Wipfli helps businesses and organizations assess their compliance with security and privacy control requirements, as well as create corrective action plans (CAPs) that align with HITRUST CSF.

A subject that frequently comes up during our work with clients is cloud computing services — in particular, whether Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) and other third-party tools offer features that can help address the assurances required across the 19 HITRUST CSF Assessment domains.

In this whitepaper, we're going to cover four specific areas related to the HITRUST CSF and the cloud:

1. Cloud platform compliance, shared responsibility and how different cloud solutions compare
2. Endpoint protection, portable media security and mobile device security
3. Audit logging and monitoring
4. Configuration management and vulnerability management

In each section, we'll share some of the useful tools and features we've encountered while performing HITRUST CSF Assessments that can help with compliance.

A couple caveats before we dive in: This will not be a comprehensive list but rather a list of constructive observations. Keep in mind that any given tool described may perform a variety of security tasks. One tool may be mentioned as being helpful for a specific domain, like encryption, and another as being helpful for endpoint protection, but this doesn't necessarily mean that either tool can't be used for either task.

WIPFLI

Information protection program: Using cloud platforms

One of the chief advantages of using AWS, Azure or GCP is that these solutions come from companies with deep resources at their disposal. Because of that, they have been able to obtain certifications in a wide variety of security standards.

While HITRUST CSF is and can be used by many organizations across many industries, the healthcare industry has been on the forefront of adopting it. Thus, HITRUST provides an industry-accepted framework that addresses many different standards and regulations, including HIPAA.

All three of the cloud providers mentioned conform on both counts. All can provide numerous certifications in support of compliance with various security frameworks, not just HITRUST CSF. Among them:

- Cloud Security Alliance (CSA)
- ISO* 9001, 27001, 27017, 27018
- FDA
- FISMA*
- HIPAA*
- NIST*
- PCI-DSS Level 1*
- GDPR*

*Frameworks that HITRUST also incorporates.

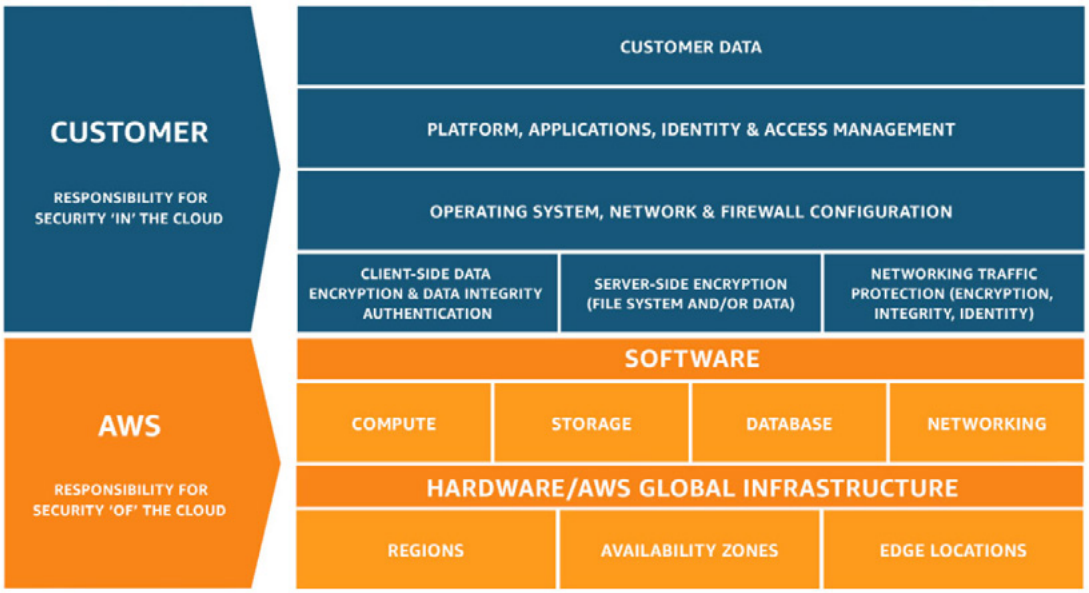
In terms of comprehensiveness, Microsoft is the leader when comparing the three different vendor sites and their list of security compliance coverage (see links below). But while Microsoft does have the greatest number of unique certifications, it is likely that many of them will not be applicable to most organizations. This is especially true if your company is in the United States.

For more information on security compliance:

- AWS: https://aws.amazon.com/compliance/services-in-scope/
- Azure: https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/
- GCP: https://cloud.google.com/security/compliance

Shared responsibility

When using cloud platforms, it's important to note that none of them can ensure all aspects of your environment are secure.In fact, under certain conditions and depending on usage of the platform, they may not be responsible for security at all. This is why all three present a "shared responsibility" model and agreement. All three of the companies give their own examples of what they consider to be their responsibilities and those of the customer. Ultimately, it is the customer that is accountable to ensure all aspects are covered.



Shared responsibility model for Amazon Web Services

Shared responsibility model for Microsoft Azure

Shared responsibility model for Google Cloud Platform

These illustrations are useful in understanding some of the pros and cons of cloud-hosted environments and solutions. As they point out, the responsibility for the security of the cloud environment changes based on whether the usage is an Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) offering.

In the shared responsibility models, when moving from IaaS to SaaS, notice that more of the security responsibility falls on the provider, yet the provider also assumes more control over customers' operations. Therefore, organizations must have much more faith in providers and their ability to keep client data and intellectual property safe.

The good news is that for any security you as the customer are responsible for, all of the cloud platforms provide plenty of tools, either directly from them or from third parties, to use in securing the environment. However, such tools do require use by someone who is knowledgeable about how to set up and manage them properly.

One important thing to note is the fact that all three cloud platforms have achieved and maintain HITRUST CSF Certification. The reason this is important is that there is the concept of "inheritance" within the HITRUST MyCSF Tool. This means it may be possible for an organization to share credit for some of the controls maintained by the cloud service provider.

For example, there is an entire domain within the HITRUST CSF framework that relates to physical security. If you were using a cloud provider to host infrastructure, you would be responsible for all physical security of that equipment. In an audit, evidence that there is physical security at the cloud data center would still need to be produced. This is normally achieved through the use of third-party security reports and audits, a walk-through or other types of vendor risk assessments.

However, if the cloud provider is HITRUST certified, it could be as simple as pointing to their certification and inheriting credit for those same controls that have already been validated and certified under the HITRUST CSF framework.

IaaS vs. PaaS vs. SaaS

Here's what each of these terms mean:

Infrastructure as a Service: IaaS is really just a virtual machine, nearly identical to buying some equipment and a rack and setting them up as an on-premise solution. The difference with IaaS is that all the components are instead purchased by the cloud service provider. These components have already been set up, and access is provided. However, the customer is still responsible for pretty much everything else, such as patching security (e.g., keeping Windows updated), managing applications, and setting up virus scanners, databases, etc. — all aspects other than buying the actual physical machines.

Platform as a Service: PaaS puts much more of the security management in the hands of the cloud-hosting provider. Here, almost all aspects of the machine itself are managed by the cloud service provider. The only thing required of customers is to deploy their applications and manage their data.

Software as a Service: With SaaS, the only thing customers must do is manage users. Think of Salesforce.com or Microsoft Office 365 as examples. They are platforms that have been set up, and customers are simply given access. For the most part, people use them "out of the box."

Cloud security

When it comes to overall cloud security compliance and management, all three of the cloud platforms offer tools to help achieve and maintain compliance.

Azure Security Center: This tool gives an organization a complete overview of its environment's security health. It allows an organization to define and enforce technical security policy. It will point out security gaps and then walk users through ways they can remediate the issues with either first-party solutions from Microsoft or solutions from a third party.

For example, if there is a firewall gap, Barracuda is available to remediate the issue if an organization believes Microsoft's solution is not adequate.

Also included with this tool is a dashboard that gives organizations insights into their environments, including suspicious or obvious malicious activity. It's important to understand, however, that this service is not a default, nor is it free. In fact, consider the following factors:

- Data collection (a setting in Azure) must be turned on. It is off by default.
- The data collection uses Azure Blob Storage, which costs money as more space is used.
- Security policies must be manually configured.
- The machine learning and security alerts used by the security center incur a cost per resource.

Click here to watch a Microsoft video introducing the Azure Security Center.

GCP Security Command Center: This service is similar in many respects to Azure's Security Center in both functionality and user interface. It gives a customer an overview of their environment and a centralized management console. The console and supporting dashboards point out issues and anomalies within the environment and send out alerts when necessary. Similar to Azure, the service will also present solutions to remediate the issues.

Click here to watch a Google video introducing the GCP Security Command Center.

AWS Security Hub: In terms of functionality to both Azure and GCP, this service provides all of the same features. However, it also adds on much more in terms of maintaining compliance within an environment. While not cheap when fully utilized, it's currently the best service when speaking to which of the cloud platforms will be the most helpful in gaining HITRUST CSF Certification.

All three of the cloud platforms have built-in security tools and also allow you to bring in third-party tools. AWS has several proprietary security tools, such as GuardDuty (intrusion detection and prevention), Inspector (automated security assessments), IAM Access Analyzer (access management), Macie (machine learning) and Firewall Manager.

Originally, these were all separate logging and monitoring functions under the AWS umbrella, but with Security Hub, the logs from all of these different tools are drawn in and analyzed holistically. Not only that, but third-party tools such as virus and vulnerability scanners can also be drawn into this tool. You can also configure centralized alerting using this tool for the single pool of logs that are now being collected.

Going even further with its offering, though, AWS Security Hub also has the ability to run continuous compliance checks against the environment using a control's framework. Similar to a HITRUST CSF Assessment, which tests a customer's environment against its controls, the security hub is continuously checking the security in place against a control's framework, such as the Center for Internet Security (CIS).

The one caveat to all of this, though, as with the other tools, is the cost. AWS Security Hub has been introduced at a fairly modest price point based on usage. However, this does not factor in the cost of all the other tools that are feeding into Security Hub. As mentioned before, there are the AWS proprietary tools as well as third-party tools, and all of them incur a cost in and of themselves.

Click here to watch an Amazon video introducing AWS Security Hub.

Comparing AWS, Azure and GCP*

Beyond the security offerings of each tool, here are some points of comparison for each of the cloud platforms:

Capabilities	Amazon Web Services	Google Cloud Platform	Microsoft Azure
Provides IaaS, storage and networking capabilities in the cloud.	✓	✓	✓
Provides the essential tools needed for setting up and managing an enterprise cloud environment.	✓	✓	✓
Can spin up Windows, Linux and other open-source environments and databases.	✓	✓	✓
Can bring in third-party tools for use in the environment.	✓	✓	✓
Has the most products overall and more commercial products available.	✓		✓
Is more platform agnostic and focused on open-source technologies, fully cloud-based companies and mobility.		✓	
Provides native backup and archive service.	✓		✓

Currently, GCP is the cheapest option when comparing what is needed at the most basic level to set up a cloud environment. AWS is the most expensive. However, this will likely change over time as the three companies continue to compete with one another.

For a small start-up company, GCP may be the best option because it is the cheapest and because of its focus on open source. Open-source tools cost less to utilize (in many cases, they are free).

If your organization is already a Microsoft shop, Azure will make the most sense because Microsoft itself is the developer of the tools and services already being used. By adding in Azure, discounts and bundles will be available. Also, the transition from on premises to the cloud will be much more seamless, since most of Microsoft's tools and services are already integrated with Azure.

For a company looking for the most features, both from environment and security standpoints, and regardless of the cost, AWS may be the best choice.

*Observations in this section were made by comparing each of the Cloud providers' websites and marketplaces. Links below:

AWS Marketplace: https://aws.amazon.com/marketplace/
Microsoft Azure Marketplace: https://azuremarketplace.microsoft.com/en-us/marketplace/
Google Cloud Platform Marketplace: https://cloud.google.com/marketplace/

Honorable mention: Salesforce Platform

One other cloud platform to mention is the Salesforce Platform cloud service. The reason it was not included with the other three is that it is not a full environment or enterprise solution. The platform is focused mainly on application development in a PaaS offering (see link below for details).

Salesforce handles all of the back-end infrastructure, including the automatic generation of storage databases, and even some of the front end, by generating developer console user interfaces to write code with. The platform can be connected to whatever code repository is currently being used by an organization. In terms of security, Salesforce also maintains a very high level of compliance, including HITRUST CSF Certification, similar to the big three above.

Click here for more information on Salesforce security compliance, and click here for information on the platform itself.

Endpoint protection, portable media security and mobile device security

Now that we've covered some of the top cloud platforms in detail, let's dive deeper into HITRUST and the cloud. In this section, we're going to focus on the HITRUST CSF Assessment domains of endpoint protection, portable media security and mobile device security.

Domain: Endpoint protection

When it comes to centrally managed virus scanning and anti-malware tools, there's an abundance of options available from a wide variety of vendors. Endpoint protection is needed for both servers in the cloud and on premises, as well as endpoints such as laptops and desktops used in the workplace.

All endpoint protection suites strive for the same goal: to protect endpoints from malware and exploitation. Given the speed at which new schemes and technologies emerge, on any given day, one vender could pass another to become the "best" protection available. With that in mind, here are some examples of solutions that we frequently come across while doing consulting and auditing work:

- Microsoft System Center
- Trend Micro
- Symantec
- McAfee
- Malwarebytes
- Webroot
- Kaspersky
- CrowdStrike

For HITRUST, the single most important factor in the endpoint protection domain is that a solution is installed, operating and updated on a regular basis.

Other requirements are: 1) the availability of audit logs that show scans are occurring and that malicious code is being blocked, 2) a console to show central endpoint management and 3) the ability to produce detailed reports.

When it comes to these primary factors, all of the vendors above deliver what's needed. In fact, all actually go above and beyond by addressing today's specific concerns and operating environments, and they all can be used in a cloud environment.

Therefore, security is being advertised related to four key areas: endpoints, networking, internet and servers. Each vendor describes these areas slightly differently, but in essence they are the same four areas.

For endpoints, networking and servers, more traditional levels of protection — including malware scanning, protection against unauthorized access and scans for attackers in the system — are available.

Because phishing attacks and ransomware are on the rise in today's environments, it's no surprise that a big advertising point on all vendors' sites is how they'll protect an organization from rogue URLs, attachments and other elements that can lead to ransomware and social engineering.

Most of the big-name vendors provide similar levels and varieties of protection, so how do you choose the right one for your organization? There's cost, of course, but also consider interface (things like the management console and dashboards available), ease of use, how the solution could interface and/or interfere with other applications and, if applicable, how it performs in a cloud environment.

Domain: Portable media security

When it comes to portable media security, the simplest solution would be to just not allow portable devices to be used. This approach may not be practical or possible, though, particularly since there is still a need in organizations to use devices like flash drives or other portable storage media.

The good news is that if an organization is already using Microsoft products on an enterprise level, BitLocker is included. BitLocker is Microsoft's product for endpoint encryption and can be used to encrypt storage devices connected to an endpoint. You can further automate this protective measure by combining the feature with group policies set up in Active Directory. For example, through group policy it is possible to not allow portable storage at all, to enable read only, or to enforce encryption if someone tries to write data to a device.

Beyond Microsoft's built-in solution, there are other enterprise solutions that can work with BitLocker or be used by themselves. They include not only encryption but also centralized management and control.

One particular product is Sophos Safeguard. The product advertises full disk encryption for all the major formats, including NTFS, FAT and FAT32.

For organizations looking for a tool that goes further than BitLocker, Safeguard offers some more comprehensive features. First, it offers an option to select, manage, and authorize which users can view encrypted data, even in the event the hard drive/portable storage is removed/moved. Second, it has the ability to silently encrypt and to encrypt only specific file paths.

Safeguard also includes tools to centrally manage all endpoints and devices running the solution. In addition, it delivers other features important for HITRUST compliance, including remote encryption, whitelisting for access, a dashboard and device tracking.

Domain: Mobile device security

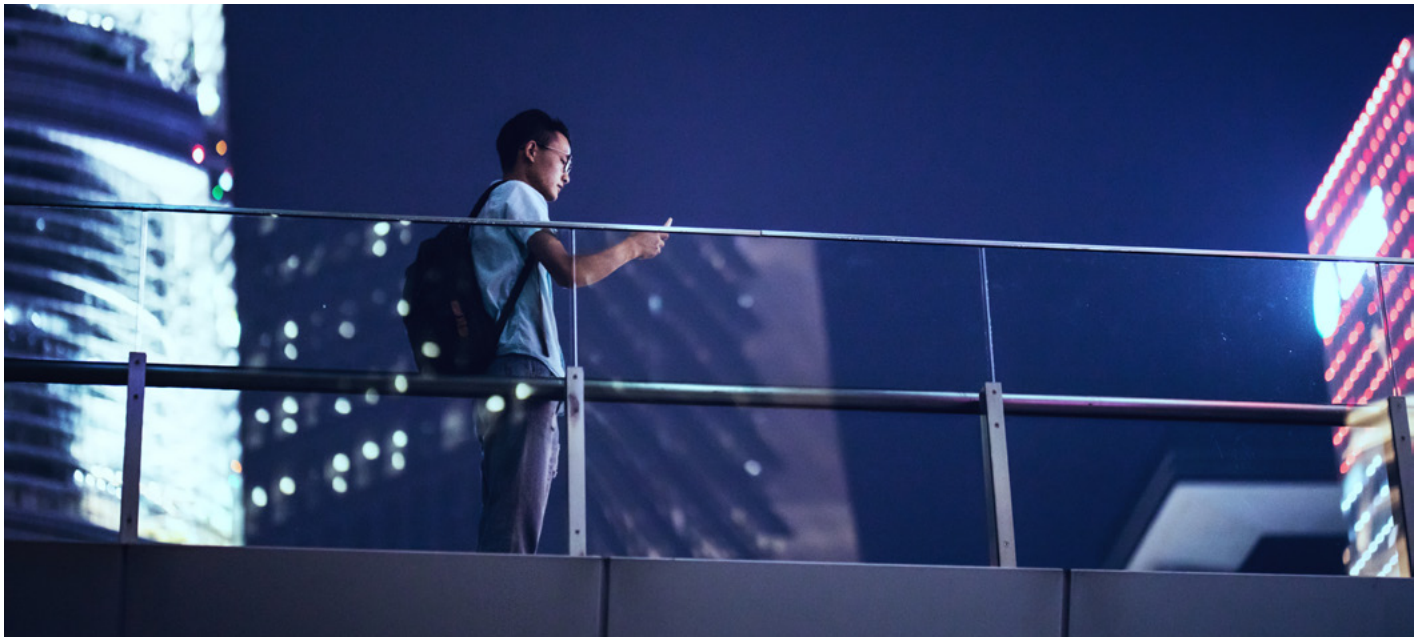
One of this HITRUST domain's more comprehensive requirements is that mobile computing devices be protected at all times by access controls, usage restrictions, connection requirements, encryption, virus protections, host-based firewalls, secure configuration and physical protections.

This is really an all-encompassing statement about the technical management and control of all endpoints and mobile devices. Each element, from access controls through physical protections, is covered by measures taken in other HITRUST domains.

Still, good tools are available to support mobile device management (MDM), particularly in bring your own device (BYOD) environments. Because of the rise of personal smartphones and the decline of corporate-assigned devices, many organizations must now consider how best to monitor and control personal devices that are within their somewhat limited scope of control.

The following tools aren't intrusive (but can be if that is desired) yet still protect the organization. They can also be considered for use with corporately owned devices as well.

VMware Workspace One (formerly known as Airwatch): The platform offers management tools for overall MDM, BYOD, mobile security, mobile applications, email, browsing, laptops, and identity, to name a few. With the MDM console, an organization can also track and monitor all enrolled devices. An enrolled device can be completely wiped in the event it is stolen or can be enterprise wiped (removing organization data only) in the event an employee quits or is terminated.



JAMF: JAMF is an MDM platform specifically geared towards the Apple platform, including iPhones, iPads and other Mac devices. During our consulting and audit work, this product has been popping up more and more lately as organizations are opting not to use Windows-based workstations and infrastructure. The platform is available to use from the cloud or can be installed on premises. Features include: device content management (whitelists and blacklists), access control, up-to-date asset listings and tracking, and (similar to Workspace One) the ability to remote wipe.

In addition to these features, JAMF Pro has application programming interfaces (APIs) available to integrate with other products through custom integration, and the data from the platform can be shared with Microsoft's System Center Configuration Manager (SCCM).

Other products that could be considered for MDM are Microsoft Intune, Cisco Meraki and SOTI. However, as mentioned earlier, many of the major security tool vendors are offering some form of MDM at this point, so always check first whether a bundle is available from an existing vendor.

Audit logging and monitoring

When it comes to the HITRUST CSF domain of audit logging and monitoring, there are quite a few potentially beneficial compliance tools your organization can use.

In fact, audit logging and monitoring tools are available in vast quantities. There are tools to monitor applications, logs, servers, cloud environment health, users, email and more. There are also tools available for security information and event management (SIEM), which take data from all of the above-mentioned audit logging and monitoring tools, bring all of that data together, correlate events and produce manageable analysis workloads.

Here are some key insights into the most prevalent solutions available:

Amazon Web Services, Microsoft Azure and Google Cloud Platform: As mentioned in the first section of this paper, all three of these cloud platforms include basic audit logging and monitoring capabilities at the entry cost. Included is information for uptime, performance, alerts and other environment health statistics. More robust logging is available for an additional cost.

Related specifically to AWS Security Hub, Amazon has also published a list of available third-party integrations. Any product that shows up on this list will be able to integrate easily with the Security Hub and be able to send, receive or do both for the logs. Click here for more information on the available integrations.

Splunk: This is by far the most common SIEM tool we come across during our consulting engagements. It is also one of the most robust SIEM tools (but also the most expensive). Splunk offers modules related to IT operations, app analytics, breach analysis, insider threat, business analytics, and internet of things.

The main selling point is that this product can produce data that can help prevent issues before they even occur, or if they are already occurring, the data collected will point out the issue at the earliest possible point.

Splunk can also collect logs from almost any platform — including applications, infrastructure and networking devices — and then put them in a central location and allow filtering, reporting and all types of analytics. Splunk also includes AI and machine-learning capabilities that will adapt to the data running through it and result in a better and more tuned monitoring program.

LogRhythm: Similar in scope to Splunk, LogRhythm contains a variety of monitoring modules with the capacity to bring all the data together to determine whether bigger issues are at hand. Other logs from outside LogRhythm can also be fed into this tool for analytics and correlation.

Among the modules LogRhythm offers are threat management, user behavior analytics, network threat detection, endpoint threat detection, cybercrime detection, threat intelligence, honeypot and deceptive analytics, file integrity monitoring, and a security operations center.

While this product offers a wide variety of services, there is also significant cost associated with using all or most of them.

AT&T Cybersecurity: This product is also considered a SIEM solution. In addition to its vulnerability management features, it can be leveraged for event correlation. So while it monitors for things like asset discovery and inventory, possible intrusions, net flow and vulnerabilities, it also will bring all of that data together and determine whether there is some relation and whether a bigger issue is occurring. All other organizational logs can be fed into this tool for correlation and analysis as well.

New Relic: This product includes modules for monitoring applications, synthetics (software workflow monitoring), web apps, servers and mobile apps. It also has a module called Insights that collects data from all of the above-mentioned components and brings the data together for focused analytics. So it acts much like a SIEM tool, but solely for the New Relic environment.

Paladion AI.saac: This tool is advertised as the next evolution in SIEM tools — for good reason. While most of the SIEMs above will collect data and do threat analysis, AI.saac also has the ability to perform threat anticipation by ingesting and analyzing numerous threat feeds. It also performs active threat hunting, which involves searching for and preventing zero-day issues.

These are reasons why Wipfli is in partnership with Paladion and provides managed services with this product. Services include the setup and management of this tool across an organization's enterprise environment, as well as being the incident response team for any issues that come up.

Other tools: HP's Arcsight, SolarWinds, IBM's Qradar, SumoLogic and McAfee ESM are all advertised as SIEM tools. When considering any of these options, however, it's essential to know your security objectives and perform the research necessary to ensure the selected product will be a good fit.

Configuration management and vulnerability management

We've explored potential solutions that support five of the 19 HITRUST CSF Assessment domains. Our final section of this paper dives into another two domains: configuration management and vulnerability management.

Configuration management

The configuration management domain is not inherently technical in nature. There is a lot of policy, procedure, collaboration, review and approval involved. Yet tools can be used in this domain to help with management and compliance.

Software configuration management (SCM) tools are part of the larger cross-disciplinary field of configuration management. SCM is defined as the task of tracking and controlling changes in the software.

SCM practices include revision control and the establishment of baselines. If something goes wrong, SCM can determine what was changed and who changed it. If a configuration is working well, SCM can determine how to replicate it across many hosts.

Vulnerability management

A large part of this domain addresses vulnerability testing and management. There are abundant third-party vendors available to perform vulnerability/penetration testing on an organization's environment (including Wipfli), but there are also tools available so an organization can do some of this testing on its own or use a completely managed security solution.

Since vulnerability management is so large in scope and includes a variety of different security subjects, the tool descriptions that follow likewise provide for a variety of different uses and features.

How CSM tools help meet HITRUST configuration management requirements

There are several tools available to help automate the configuration management process, which used to be highly manual. Tools like Ansible, CFEngine, Puppet, Chef and Jenkins all provide a different graphical user interface and a slightly different spin on offerings, but they all in some form or another provide features that help fulfill HITRUST CSF requirements.

- Allows administrators, developers and testers to run automation jobs at the push of a button against multiple test environments.
- Automates configuration management, application deployment and configuration of tasks across an IT environment.
- Can be used to deploy testing environments with specific configurations.
- Offers secure user management to allow automation testing against an environment a user has access to.
- Logs and audits everything for reporting and review purposes.
- Includes built-in communication and survey features so any new code will go through the correct approval and chain-of-custody steps before production deployment.
- Can be used to manage current versions of software/systems and archive older versions if recovery or review is needed.
- Can be used to keep code organized and appropriately labeled for easier collaboration between development and operations teams.
- Ensures the organizationally defined configuration standard is always the actual state on the managed endpoints.

Microsoft Azure: Microsoft has partnered with the third party Qualys to provide an integrated vulnerability scanning solution. The Qualys scanner is part of the Azure Security Center. It is available at the "standard" pricing tier and higher, and no separate account or license with Qualys is required to use this feature.

AWS: AWS has an add-on called Amazon Inspector. It's advertised as being an automated security assessment service that can help identify and remediate security issues (similar to the Azure offering). This service can also be used in combination with other services under the AWS Security Hub.

In addition, many of the third-party vulnerability scanning solutions available will work in a cloud environment. Here is a brief summary for a few of them:

Tenable: Tenable is the most common vulnerability scanning and management tool we come across while doing HITRUST CSF Assessments. Tenable.io is advertised as being able to scan for vulnerabilities, advanced threats, web application security and compliance violations.

Alert Logic: This solution offers two products: Alert Logic Cloud Defender and Alert Logic Cloud Insight. Both are designed to work in a cloud environment.

Qualys Cloud Platform: This offering gives a continuous view of security and compliance related to asset discovery, network security, web app security, threat protection and compliance monitoring. It advertises native integrations for AWS, Azure and GCP.

AT&T Cybersecurity: Like many other offerings we've covered, this is a diverse suite. For vulnerability management, the solution offers a tool called AT&T Unified Security Management Platform, which contains a built-in vulnerability assessment tool and helps identify vulnerabilities, provides detailed reports on its findings and helps with remediation. It also includes an asset discovery similar to the Qualys product, along with scanning and reporting features on demand.

Some other products that are worth mentioning for comparison are: ManageEngine, Rapid7 and Tripwire IP360.

Cloud-powered compliance

As cloud computing becomes a more commonplace approach for securing data, using third-party tools can help organizations address HITRUST compliance and meet the assurances required across the 19 HITRUST CSF Assessment domains.

Which tools your organization chooses to use are highly dependent on your needs, your budget, what technologies you already use and what current processes you have for meeting HITRUST requirements.

In this paper, to help answer questions about HITRUST requirements related to the cloud, we've covered 7 of the 19 domains, as well as the third-party tools that can help with compliance. As a HITRUST Authorized External Assessor, we can answer any questions you may have about requirements for the other CSF assessment domains, plus questions about the tools we covered or the HITRUST CSF requirements we mentioned.

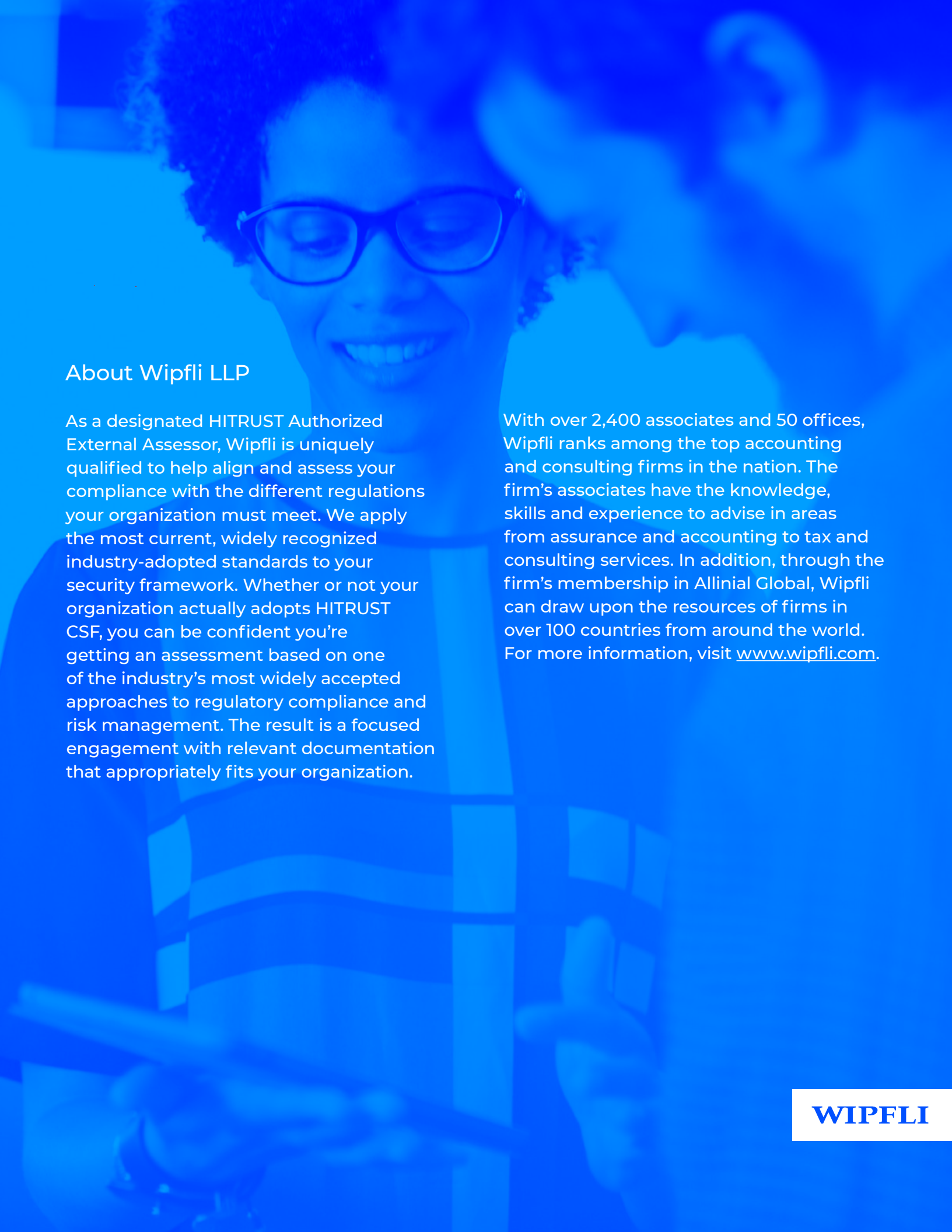
Contact us to learn more about how we can assist your organization with performing a HITRUST CSF Assessment, choosing the right technology tools to assist with compliance, or assessing your security and privacy controls in preparation for starting the HITRUST CSF Certification process.

Additional resources

Common misconceptions from a HITRUST Authorized External Assessor

The business associate's path to HITRUST CSF Certification

HITRUST vs HIPAA: What is the difference?



About Wipfli LLP

As a designated HITRUST Authorized External Assessor, Wipfli is uniquely qualified to help align and assess your compliance with the different regulations your organization must meet. We apply the most current, widely recognized industry-adopted standards to your security framework. Whether or not your organization actually adopts HITRUST CSF, you can be confident you're getting an assessment based on one of the industry's most widely accepted approaches to regulatory compliance and risk management. The result is a focused engagement with relevant documentation that appropriately fits your organization.

With over 2,400 associates and 50 offices, Wipfli ranks among the top accounting and consulting firms in the nation. The firm's associates have the knowledge, skills and experience to advise in areas from assurance and accounting to tax and consulting services. In addition, through the firm's membership in Allinial Global, Wipfli can draw upon the resources of firms in over 100 countries from around the world. For more information, visit www.wipfli.com.

WIPFLI