WHITE PAPER

GILLIAM SECURITY

Adoption of Compliance Requirements through Continuous Compliance

Looking at compliance across the board.

Many times several different assessments are required to understand adherence to a policy, regulatory framework, industry requirement, or some other regulation. While none of this difficult, it can result in asking the same question multiple times or fatigue of your auditee.

To reduce fatigue and be able to view compliance across the board, as well as plan for future requirements, an organization needs to establish an *enterprise security architecture*.

What is Enterprise Security Architecture

Enterprise security architecture is the set of controls, policies, standards and procedures that govern security in an organization. This is *different* from solutions architecture in that solutions architects creates requirements based on what is outlined in the enterprise security architecture, commonly referred to as patterns.

For example, the solutions architect would recognize the patterns established by the enterprise architectures as the methods available to "build" from. For example, the pattern for authentication may be SAML2.0 and OAUTH2 for authentication within an environment. The upstream governance of this requirement would be the:

- The control. In this case, "Strong authentication protocols are used for authentication of systems within the environment."
- The policy would state, "Strong authentication measures *shall* be used for authentication of systems within the environment."
- The standard would read "Strong authentication, to include SAML2.0 and OAUTH2, should be used as methods for authentication of systems within the environment."

Why Does Security Assurance Care

Several different standards require the use of strong authentication. As a security assurance professional in a B2B ("Business to Business") and a B2C ("Business to Customer") organization, for example, one may find that regular audits happen based on the PCI DSS (link), COBIT (link), NIST CSF (link), CIS Critical Security Controls (link) and ISO 27001 (link).

Consequently, this would result in understanding the compliance of the same control across five standards, not to mention things like Sarbanes-Oxley or other regulatory requirements that are passed down to the information security organization.

How to Solve Five for One

In order to look at security from a wholistic view to prevent fatigue of the auditee as well as have oversight of risk, risk must be evaluated from a wholistic point of view. Similar to security operations, one will not just look at a singular system, rather the impact should the system be compromised or attacked. In the compliance realm, this is where I use the phrase *Continuous Compliance*.

Let's use the need for an information security policy as an example:

- *Step 1: Understand the risk at hand.*

  ECC Council published an article in September 2020 that 88 Percent of security breaches are due to human error. That is a scary statistic. How do we fix that? We should probably create a security control to regulate what can and cannot be done.

- *Step 2: Understand what is the control.*

  We have established the need for a control to address the risk the human presents when it comes to security breaches. Let's make a sample:

  A security policy is in place and understood by employees year through annual review, approval and awareness updates.

- *Step 3: Understand the policy that addresses the control.*

  A policy is not a policy for no reason. It is based on a risk that resulted in control to mitigate a risk that in turn prompted the need for a policy statement to address the control and ultimately mitigate the risk, hence the need for a *risk acceptance* for when a policy is violated.

  For example, let's look at a sample policy statement:

  ACME Information Security Policy
  Section 1.0 Approved Information Security Policy
  An information security policy shall be reviewed and approved by management at least annually.

  What is the actual requirement?
  Security policy… defined… approved… management… at least annually.

- *Step 4: Find a common point to reference this requirement.*

  Typically, my recommendation would be to focus on an industry recognized framework so one can work up to be more granular. For example, I typically use ISO 27001.

  That said, let's understand where this aligns in ISO 27001. … Found one!

  A.5.1.1 Policies for Information Security
  A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

- *Step 5: Understand how this is validated by understand the audit procedure behind the control.*

  For example, let's use one below:

  1. Validate a meeting took place to review the information security policy in the last 12 months.
  2. Inspect the information security policy to ensure the approval by management in the 12 months.
  3. Request and review the security training curriculum to validate awareness of the updated policy was given to employees and relevant third parties in the last 12 months.

     (This just a sample, note a real audit procedure would be a lot more detailed)

- *Step 6: Understand the requirement, along with the risk as well as how it is validated, to be able to evaluate other frameworks to enable and interpret what requirement meet this same the policy as well as audit requirement along the same audit procedure and same risk. (Forgive the run-on sentence.)*

That said, let's use the PCI DSS as an example. Searching… searching… found one! Wow, there is a lot…

Requirement 1.5, Requirement 2.5, Requirement 3.7, Requirement 4.3, Requirement 5.4, Requirement 6.7, Requirement 7.3, Requirement 8.8, Requirement 9.10, Requirement 11.6, and Requirement 12.1

For grins, let's do one more: the NIST Cybersecurity Framework. Searching… searching…

ID.GV-1: Organizational cybersecurity policy is established and communicated.

Result of Continuous Compliance

Here is a sample benefit of what is provided by performing this kind of analysis:

> ***ACME Information Security Policy***
> ***Section 1.0 Approved Information Security Policy***
> *An information security policy shall be reviewed and approved by management at least annually.*
> ***Related Requirements:***
>
> - *ISO 27001: A.5.1.1*
> - *PCI DSS v.3.2.1: 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 11.6, 12.1*
> - *NIST Cybersecurity Framework: ID.GV-1*

Now when you are looking for evidence, mark evidence to show what ALL the requirements are it applies to. As part of this, when one wants to look at NIST Cybersecurity Framework compliance based on ISO compliance, you can have a quick view.

What to Watch For

One thing to keep in mind has you work this is make sure scope for each of these areas of compliance is the same. If this is not done, it could be a bigger nightmare than if nothing was in place at all.

Need Help Setting Things Up?

Have questions or need help? Contact Gilliam Security. We have mapped 20 of the industry regulations, frameworks and regulatory requirements from ISO 27001 to the General Data Protection Regulation to PCI DSS v3.2.1.

Why Gilliam Security?

Gilliam Security has recognized consultants from major fortune 500 companies with certifications such as the CISSP, CISM, CISA and CRSIC. Each consultant also has experience in building the information security, as well as privacy, function from inception to maintaining operations.

Contact Us Today at sales@gilliamsecurity.com