CREATE A SUSTAINABLE CYBERSECURITY PROGRAM WITH SECURITY CONTROL FRAMEWORKS

Build a Control-Centered Universe for Next-Level Cybersecurity Program Management

ProcessUnity

PROCESSUNITY WHITE PAPER

INTRODUCTION

Whether you're a CISO that needs to support compliance efforts, or an internal assessor tasked with evaluating controls, maximizing the effectiveness of a cybersecurity program can be challenging. Often there are many moving parts within a cybersecurity program – regulations, high-value assets, third parties, threats and their respective downstream owners – making it difficult to achieve a genuine sense of your cybersecurity risk. How can you ensure that your controls adequately meet security objectives to protect your high-value assets and prove compliance?

Enter cybersecurity control frameworks. Control frameworks exist to provide your program with the tools to effectively identify, manage and respond to risks across the extended enterprise. How you decide to use these frameworks can determine your program's success. With maturity and resources considered, programs can meet their cybersecurity objectives by mapping existing controls to industry- and regulatory-relevant frameworks or leveraging a metaframework with pre-built mappings across regulations.

Industry-relevant frameworks offer a recognized library of controls for organizations to standardize their security practices with. These standard frameworks, which are typically government or industry-backed, focus strictly on cybersecurity. Conversely, a metaframework is a comprehensive control set that maps to multiple industry frameworks and regulations. A metaframework will reduce the tedious work of compliance and add value by identifying security and compliance gaps across standards and regulations, delivering assessment clarity, and streamlining reporting – without a heavy investment of valuable resources.

We'll review the criteria for selecting the appropriate framework for your organization then cover how to build your program around it for lasting success.

This paper will take a step-by-step approach to mapping internal security controls to the cybersecurity framework of your choice.

CONTENTS

ProcessUnity

1.

ORGANIZE YOUR RISKS, ASSETS, THIRD PARTIES AND OWNERS

In order to build a strong foundation for your program, it's essential to first develop a wholistic view of your organization's key threat areas: known risks, third parties and key assets.

Identify Risks

Every organization faces a unique risk landscape based on factors specific to them: industry focus, company size and third-party relationships, to name a few. Establishing clear visibility across the extended enterprise is the first step in mitigating risk from all angles. Your organization should compile information on every possible area for risk exposure. This will entail reviewing IT infrastructure, applications and employee networks in the context of their value and the data they harbor. Remember to assess your risk both internally and externally.

Identify Assets

Identify your organization's crown jewels or high-value assets to evaluate where they stand in your risk landscape and how you can protect them. Document every application, including the data they pertain to and their owners. Establish a clear understanding program-wide of each asset's exact value to your organization.

Identify Third Parties

Begin by creating an inventory of every third party your organization deals with. Take stock of what data and assets your organization's third parties can access and the value the third party brings. Later, you'll assess each third party's security practices to understand how well organizational data are protected.

Finally, these key risk areas should be assessed, tiered and grouped based on criticality. Depending on the value of the data they protect or have access to, certain assets and third parties will need more stringent controls. Determining your organization's risk exposure will enable your program to map it to the proper control within a framework and appropriately schedule control reviews.

Identify Owners

In organizing your business data, you will need to identify the owners of risks, assets and third parties within your organization. Doing so will ensure that those accountable understand their specific roles and associated responsibilities while helping to keep track of the influences on controls. Every risk, asset, third party, and control should tie back to an owner that can provide valuable performance insights. This promotes cyber accountability across the organization and involves those who are invested from a business perspective to get involved in how cyber risk is managed.

2.

IDENTIFY YOUR CONTROLS

Be it internal or external, every risk identified in your organization will require a mitigating control. Depending on your program's maturity, it may or may not operate with an existing set of controls. To adequately assess your control posture, consider:

- Does your organization have a pre-established set of controls?
- If you have existing controls, are they already mapped to a relevant framework? How well do they satisfy the standards set by the framework?
- Do you have existing documentation of your controls?

To ensure that your organization covers all its regulatory bases, your controls will need to align with an industry or government standard framework. Whether or not you have defined controls, a framework will help your organization improve existing controls to standardize your cybersecurity program and ensure that everyone involved in the program is on the same page concerning security requirements and objectives. Choosing the right framework to help your program meet its goals will require an understanding of your organization's size, industry focus, asset types and more.

There are three major cybersecurity frameworks with which most companies align their programs:

1. **ISO 27001**
   ISO 27001 is a series of best practice controls related to protecting information security. It includes information security management system requirements and defines the main focus areas in building a security program. It offers externally assessed certified.
2. **NIST CSF**
   NIST CSF is a voluntary framework for mitigating cybersecurity risk in critical infrastructure organizations, such as governmental entities like the Department of Defense. It is based on existing standards, guidelines, and practices that are flexible enough to be implemented by non-governmental and non-critical infrastructure agencies.
3. **NIST 800-53**
   NIST 800-53 recommends controls for all US federal information systems. The guidelines take a multi-tiered approach that breaks controls into three categories based on severity.

The above frameworks rarely serve as a "one-size-fits-all" approach for compliance. Programs will likely need to add controls from various frameworks based on their unique compliance requirements. For example, programs may need to augment their framework in accordance with regulations such as GDPR, CCPA and PCI DSS. Organizations should consult with a legal team to ascertain their specific regulatory requirements.

Once you have a clear understanding of which framework is most relevant to your organization, you can decide how to proceed based on your current control posture. In the next section, we will explore options for leveraging the SCF metaframework or manually mapping your program.

Getting Started with Controls: The Secure Controls Framework (SCF)

If your program does not yet have controls in place, or if your existing controls are incomplete, you'll need to establish a baseline of industry-standard controls for your program. A great place to start is the Secure Controls Framework (SCF), a metaframework that covers cybersecurity and privacy and includes 999 controls that are pre-mapped to frameworks such as NIST and ISO. Adopting a metaframework with pre-built mappings like the SCF will streamline the later stages of upstream mapping, reporting and certification. The SCF delivers maximum program value by providing a built-in approach to downstream mapping across many frameworks and regulations. Valuable features of the SCF include:

Pre-Built Mappings

The SCF is equipped with pre-built mappings that enable your program to adopt a single control that is mapped across every standard and regulation to which it applies. This allows your organization to avoid duplication by sharing controls, minimizing manual mapping to aspects of many different frameworks. For example, if your organization has compliance requirements with ISO and GDPR, the SCF maps one control to every applicable area across the two frameworks. The alternative is a tedious process that requires you to manually identify how controls can be applied across every separate requirement.

Accurate Control Assessment

The metaframework establishes a clear network of influence by tying every aspect of the program back to its controls. This allows audit teams to effortlessly assess how a control is performing in the context of its related regulations, owners and assets. Your program can efficiently respond to control improvements as needed to remain compliant and protect assets.

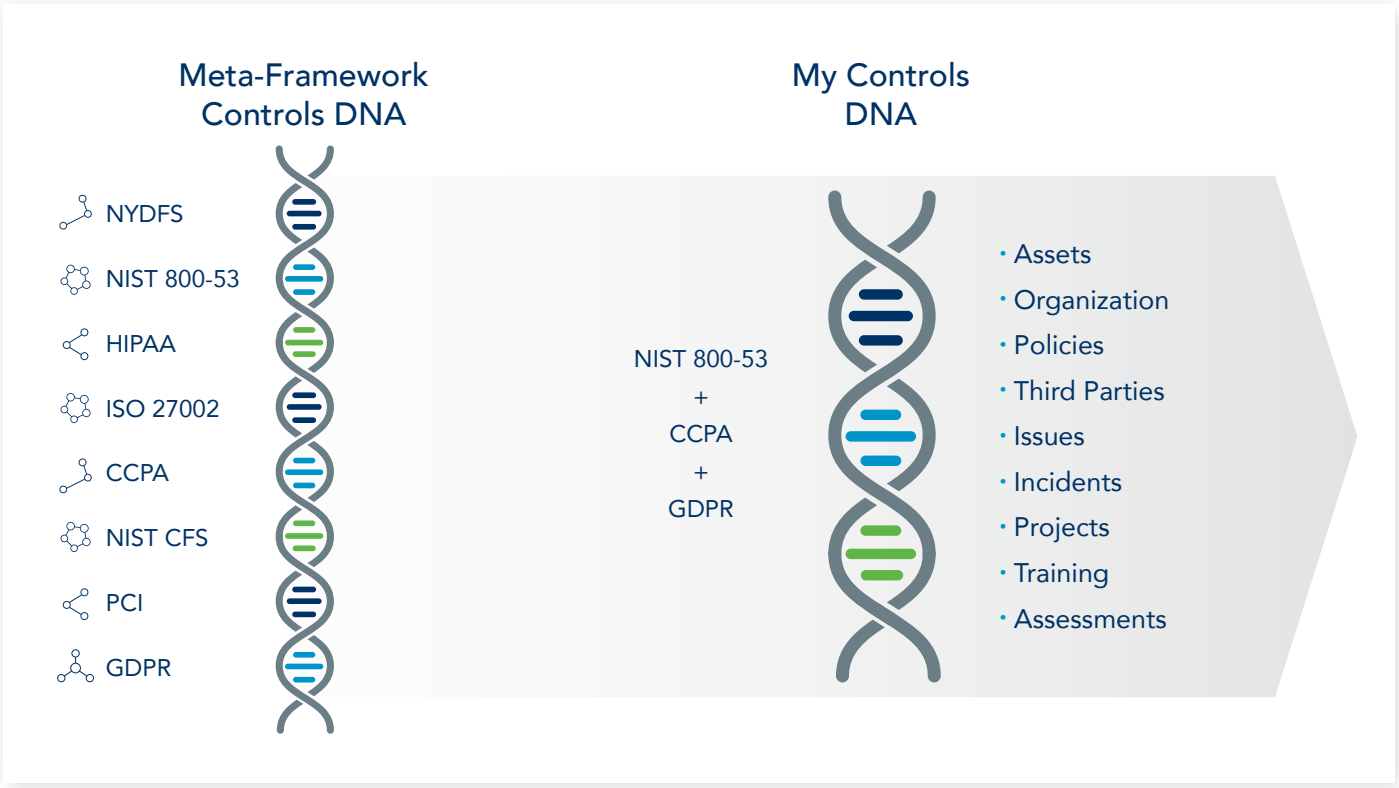
Control Gap Identification

Thanks to these pre-built downstream mappings, the metaframework naturally creates a wholistic program view that provides visibility into compliance gaps. Organizations operating within manual mapping processes often expend valuable time and resources attempting to identify and address gaps in their programs. The metaframework can be leveraged to pinpoint which standards aren't being met and thus remain compliant with ever-evolving regulations. When aligned with capable technology, the metaframework can efficiently respond to and enable policy changes across multiple controls and their owners.

Streamlined Issue Management

A high-level perspective of how controls are tied to standards, regulations and business data is extremely beneficial in the event of a security incident. Should an issue arise, the metaframework can outline the security measures that the organization has in place. Additionally, it can help identify gaps in the security posture that the program needs to address to prevent future incidents.

Cybersecurity program management is a control-centered universe – that's why the SCF is a smart, efficient choice for programs. It allows you to quickly identify the controls that apply to your organization and automatically maps each control to every standard or regulation it can apply to. The beauty of a metaframework is in the "map once, satisfy many" approach: instead of attempting to manually map a pre-existing control set across many different regulations, the SCF can be leveraged to prove and assist in compliance with a variety of requirements - all in tandem with an organization's business data.



Cybersecurity frameworks and regulations are integrated into the metaframework to be mapped to controls and organizational data.

Working with Existing Controls: Standard Framework

If your program already has a satisfactory control set, you can consider mapping them to a control framework like NIST or ISO. Then, you can determine additional controls that need to be added based on outside regulations like GDPR and CCPA for full coverage. Programs may opt to align with a standard framework because they are familiar, proven and highly regarded in their industry. However, these frameworks do not provide mapping to regulations and other industry standards that your organization is beholden to. This difference can make it difficult to streamline your controls and ensure compliance.

Whereas the metaframework leverages pre-built mappings to avoid duplication in your control set, operating without a metaframework will require you to manage controls across several regulations and standards. This less efficient approach often leads to a duplication of controls to manage against certifications or regulations.

No matter which path you choose – metaframework or standard framework – you'll need to assign control ownership within your organization. Each control should be paired with a specific owner that can accurately report on control performance.

Once you have decided on a control set, it's a useful tactic to group controls by risk domain within your organization. Since one control can be applied across different regulations and applications, categorizing risks and controls is the most efficient approach to mapping across various requirements. The SCF controls cover 32 risk domains, from Asset Management to Web Security. These controls are in place to help mitigate risks related to specific security areas. A few examples of risks within Asset Management include:

Inability to maintain individual accountability

Improper assignment of privileged functions

Privilege escalation

Unauthorized Access

Suppose you have a specific set of controls for your organization that are tied to risks within the Asset Management domain. Grouping these controls will allow you to have complete coverage over "Access Control" risks for both application owners and third-party relationships. This control set can then be used to satisfy requirements from SOC II, ISO and NIST. Ultimately, grouping your controls streamlines the number of controls needed and eliminates the burden of maintaining multiple control sets.

3.

MAP CONTROLS

Your business data and controls are organized – now your program is prepared to connect the dots with multidiscipline mapping.

Downstream Mapping (Mapping to Regulations & Standards)

Programs that opt to align their program with a cybersecurity framework like NIST or ISO will need to manually map their control set to regulations outside their main framework. This is a "check-the-box" process to ensure that the program has a control to satisfy every regulation and standard they are beholden to. Managing compliance with evolving regulations and responding to risks may be difficult for programs operating with this manual process, but it can be done if managed well.

Since the SCF features pre-built mappings, the metaframework alleviates the burden of downstream mapping. Your program can leverage the SCF to accurately pinpoint compliance efforts across multiple standards and regulations through the lens of a single control. Note that your program will need to map any pre-existing controls outside of the SCF manually.

Upstream Mapping (Your Organizational Data)

Regardless of whether your program has chosen to adopt a metaframework or a standard framework, your organizational data will need to be mapped to your control set. Mapping your risks, assets, third parties and owners to your controls will create a clear line of sight for compliance. This lends your program the agility to remain compliant with regulatory changes and respond to security issues as they arise.

Each control should be mapped to its respective risk, asset, third party and owner in the same way that they map to standards and regulations. The earlier stages of grouping your business data by criticality can be valuable to ascertain precisely where specific controls need to be implemented. Upstream mapping provides your program with a complete perspective on everything influencing a control come time for assessment. The next section will explore how to leverage the assessments of your controls and business data for maximum program insight.

Your control framework is mapped both upstream and downstream to your organizational data.

4.

ASSESS CONTROLS

Evaluating a control for effectiveness is an integral aspect of cybersecurity program management – after all, you'll want to regularly confirm that your security measures are airtight. Testing controls will determine if they are correctly implemented and within the scope of cybersecurity standards and regulations. Before you can start with this, however, you'll need to assess your business data for a realistic story of a control's performance.

Assess Business Data

The first step in assessing your business data and controls is establishing an assessment process that delivers clarity on performance and effectiveness. While there are many technologies that can be applied to identify vulnerabilities and apply corrective actions, assessments are critical in gathering business context for existing cybersecurity risk.

A questionnaire-based approach is the most effective way to gather data on the applications and third parties that rely on a control. Questionnaires should tie every question back to a control to provide complete visibility into the control's performance. Asset owners should be given a series of questions prompting them to report on internal security performance with evidence. Assessment results can then be evaluated against a series of preferred responses. The purpose of a questionnaire-based approach is two-fold: it allows the control reviewer to determine the performance of a control, and it lends insight into what is influencing that performance, giving you the best idea of how to optimize it.

Similarly, third parties should complete a questionnaire that confirms their compliance and security practices align with the organization's standards. The questions must be designed to offer the control reviewer the most information possible to assess the effectiveness of the third party's practices adequately. The control reviewer will need to save the assessment results in a centralized platform for easy reference when it comes time to report.

Assess Controls

Once your assets and third parties have been evaluated, you can assess your controls with a broader perspective of their performance.

Control owners should be given a questionnaire backed by a set of preferred responses. Like the assessment process for business data, the questionnaire must be designed to provide the maximum information on a control's performance. Then, the evaluation results can be reviewed with the results from an assessment of a control's respective asset or third party. The assessment process should provide a complete picture of how the program can optimize their control set.

Finally, your program will need to support an ongoing review process by scheduling regular assessments. Not every control, third party and asset will need to be reviewed with the same frequency. Leverage the previous stages of categorizing by risk criticality to determine how often a control, third party or asset should be reviewed. Assessment results can inform this decision as well. Depending on a third party or asset owner's responses, your program may want to assess a specific control more or less frequently.

4.

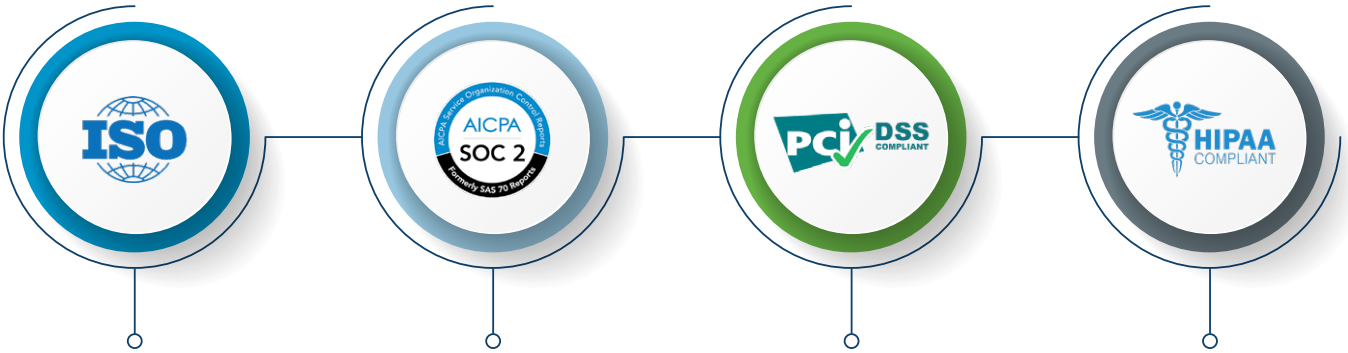
REPORTING

You've mapped internal controls to your selected framework and assessed the effectiveness of these controls – now what? Fortunately, you can use all the valuable data you have collected throughout this process to remedy any security gaps and mature your program with informed reporting. This data can be used to report on the state of organizational cybersecurity to an internal audit committee or board of directors, prove compliance to a regulatory body, inform budget decisions, and even kickstart the certification process.

Reporting is especially useful for project planning as it pinpoints the steps necessary to achieve your cybersecurity objectives. It can be used to request resources for enhancing controls or justify program decision-making.

Finally, the organized data used in reporting can accelerate certification activities. A metaframework is especially beneficial for certification as it provides a consolidation of testing and evidence gathering that can support multiple requirements, eliminating redundancy and stale data issues. Becoming certified within your chosen framework indicates program maturity and streamlines the onboarding process for future business relationships.

COMMON CERTIFICATIONS THAT ORGANIZATIONS STRIVE FOR



CONCLUSION

CISOs must understand that the key to Cybersecurity Program Management success is to center your program around your controls. Every aspect of your program- threats, risks, policies, and third parties- need to tie back to a control to ensure cybersecurity objectives are being met. The process by which you establish and manage program mapping can be made more efficient with a metaframework.

Aligning your control set to a predefined map of the requirements unique to your organization offers several benefits for your program: it cultivates enterprise-wide integration on cybersecurity objectives, delivers a wholistic view of control performance, and bolsters reporting to prove compliance and prepare for certification.

Implementing a central technology solution can accelerate your cybersecurity programs state of readiness and reduce risk and cost throughout the process. ProcessUnity Cybersecurity Program Management delivers a single, comprehensive platform for centrally managing an organization's entire cybersecurity program with prepackaged mapped content, automated workflows, assessments and dynamic reporting. The solution enables the CISO to inventory and assess high-value assets; map them to threats, risks, policies and controls; automate reviews; and capture evidence of compliance – all on a predefined schedule.

CLICK HERE TO LEARN MORE

about ProcessUnity Cybersecurity Program Management

ProcessUnity

ProcessUnity

www.processunity.com

info@processunity.com

978.451.7655

Twitter: @processunity
LinkedIn: ProcessUnity

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States