Elements of Assurance

Maximizing the Value of Framework Adoption

Frazier & Deeter

Assurance is a common buzzword in the realm of cyber security and risk management. By definition, this term relates to providing confidence in something. But in the world of cybersecurity, regulatory compliance, and risk management understanding the relevancy and meaning of this term is crucial if you intend to rely on assurances in managing risk.

The objective of this paper is to evaluate the contributing factors that dictate assurance within information security and risk management. The factors to be discussed include transparency, measurement & accuracy, consistency and integrity. But before diving in, it's important to understand the need for assurance.

The Need for Assurance

In a complex ecosystem, it is helpful to identify what assurance is and how it applies. In the digital era in which we live, it is common for organizations to be faced with regulatory challenges. For example, healthcare has HIPAA, the federal space has FISMA and FedRAMP (and soon to be CMMC) and the retail space has PCI. These regulatory challenges have been in place for many years and, for the most part, organizations have adapted.

But when regulatory obligations intersect with customer demands for data security, a new challenge emerges. Take, for example, a simple software development company. In the past, that company's information security challenges may have been limited to "doing the right thing" and "getting the biggest bang out of the budget" in an attempt to thwart off any attackers. Historically their data was limited to their employees, company-provided laptops and client/server applications that all leveraged the corporate network where the infrastructure was either on-premise or in a nearby datacenter. Today however, that same software company, in an understandable attempt to lower costs by adopting economies of scale and centralizing on their core competencies, is likely leveraging the plethora of deployment strategies collectively defined as anything as a service, or XaaS. These same organizations are also facing customer pressures to ensure their originating data is properly secured well beyond the traditional four walls of the HQ facility. In today's environment data is no longer confined within a single organization. Data flows like water through the entire supply chain and the numerous mega-breaches over the years have created a call-to-action, or what HIPAA defines as "satisfactory assurances", throughout the entire data supply chain (hence the creation of GDPR, CCPA and a plethora of state laws). This is where the challenge of maintaining information security assurances begins.

With so many frameworks, standards and guidance publications available in the marketplace, this paper will serve as a guide for evaluating the most important decision-making criteria.

Transparency

Today, organizations have many options to choose from when evaluating security and privacy frameworks that will provide the necessary assurance to support the business. Some are industry and data agnostic, such as NIST, ISO and the HITRUST CSF, while others are specific to a regulation and/or data set as with PCI and HIPAA. Regardless of the "vehicle", i.e. framework, it's important to evaluate the following:

- Adaptability and response to present-day cybersecurity threats
- Scalability in parallel to organization complexity and change
- Ability to satisfy the compliance needs of the organization
- Ability to provide reasonable internal (e.g., senior leadership, board members) and external (e.g., customers, investors) assurances based on a level of acuteness to ensure cybersecurity maturity

All of these factors drive the need for transparency.

Given the wide range of internal and external audiences, cybersecurity maturity requires a high degree of transparency. Transparency relates to several different factors, all of which are important:

1. **Framework Authorship** – When selecting a framework as the foundation of an information security program, it's important to consider the transparency that was applied when the framework was authored and as the framework is periodically updated. In short, a framework developed with industry and subject matter expert feedback provides a higher degree of applicability and trustworthiness.
2. **Framework Agnosticism** – Effective frameworks are not focused on one type of data, system or use case. Additionally, the more accepted frameworks are not focused on a specific industry. Instead, they are focused on cybersecurity maturity as a holistic and preventative measure against insider and outsider attackers. As a side benefit, holistic frameworks are flexible in that they can satisfy both risk and compliance-based purposes.
3. **Framework Availability and Comprehension** – Suffice to say, if a framework is not publicly available and cannot be understood, it's probably not well adopted. Both of these factors make implementation and ongoing maintenance simpler.
4. **Framework Precision –** Frameworks can vary dramatically in terms of the level of precision and rigor. As a comparison, the HIPAA Security Rule is comprised of approximately 55 Standards and Implementation Specifications that are loosely worded and subject to interpretation and judgment errors. The HITRUST CSF, on the other hand, scales according to organizational risk and often comprises more than 300 requirement statements that are supported by detailed illustrative procedures. Like the HITRUST CSF, frameworks should be prescriptive in nature, yet also adaptable, to counteract the multitudes of threat vectors in existence.

All of the aforementioned factors relate to the concept of transparency and should be considered with framework selection.

Measurement and Accuracy

The saying, "if you can't measure it, you can't manage it" holds true when assessing the benefits of a given framework. As is the case with most frameworks, cyber maturity is qualitative, judgment-based and lacking of metrics, KPIs or any other form of quantitative measure. As a result, maturity becomes a feeling that, when wrong, could lend itself to an unmitigated risk that becomes a target for compromise.

Factors for consideration when assessing the measurement and accuracy of a framework are as follows:

- Does the framework promote quasi-quantitative scoring measures?
- Does the framework integrate multiple maturity levels (e.g., CMMI, PRISMA)?
- Is the framework backed by detailed guidance that promotes accuracy and consistency throughout implementation and assessment?
- Does the framework define specific evaluation criteria to determine control maturity?

As cybersecurity continues to be at the forefront of concern and attack, executives, boards, customers and vendors need accurate and measurable maturity scores to continue the evolution of security within their organizations.

Consistency

Consistency is applicable to several aspects of risk management framework selection and adoption; specifically, internal consumption, external assessment and supply chain acceptance.

- **Internal effectiveness –** For a framework to be effective amongst internal constituents (e.g., compliance, information security and the business), it needs to be consistently understood and applied so that it can be consistently measured. This is easier to achieve when a framework is based on clearly defined requirements and extensive guidance that allows internal stakeholders to agree on the design and implementation of specific controls.
- **External assessment –** Frameworks are most effective when organizations can be independently assessed against them and, as an additional layer, are subject to a level of quality assurance. This promotes reliability when the assessment is complete. However, in many cases, frameworks don't require independent evaluation, trained examiners or quality assurance review. In some cases, the governing body is absent from the assessment reporting process and offers no level of approval before a certification or satisfactory report is issued. HIPAA exemplifies this as the governing body, the Office for Civil Rights, is absent from internal and external assessments. This results in a striking difference in quality and reliability in the marketplace.
- **Supply chain acceptance –** When frameworks are vague, subjective or free of maturity levels and scoring, it becomes difficult to gauge an organization's posture against that of another or even an industry baseline. This issue is compounded when assessment activities aren't subject to quality and integrity review. For example, when organizations use cybersecurity maturity as a measuring stick to evaluate vendors, a comparative evaluation becomes difficult when prospective vendors use frameworks that vary in their level of rigor, precision and quality. As a result, it is not uncommon for organizations to invest in due diligence activities that "feel right", but later find out they aren't adequate amongst the requirements of today's third-party risk management programs.

It's important to also understand that consistency doesn't just apply to assessment activities, it also applies to pre-and post-assessment activities such as system and environmental scope determination, corrective action planning and remediation activities. If any of these elements are without consideration, the reliability of the assessment and associated report is diminished.

Integrity

With the adoption of a framework and the implementation of necessary controls comes the need for assessment activities and integrity. Assessments and their report outcomes are no longer reserved for just internal audit. Report visibility extends throughout the organization (e.g., internal audit, legal, information security organization), but also beyond the organization to customers, cybersecurity insurance organizations and governing bodies (such as the OCR in the event of a breach). But if these reports don't invoke a high level of integrity, the reliability placed upon them begins to deteriorate the very assurances that they aim to provide. This brings up the question of how integrity is determined. Integrity begins when the assessing party is independent of all control activities and conforms to strict program guidelines for activities such as assessment scoping, control evaluation and scoring, control applicability, assessment frequency and quality.

Similarly, integrity breaks down when the assessing party is not properly qualified to do the assessment. Qualifications encompass having years of assessment experience, framework experience and the necessary certifications to do a high-quality/high-integrity level of work.

Simply put, the promotion of integrity starts when the adopted framework is independently assessed by an individual or organization that conforms and complies to a rigorous program that instills consistency, quality and…integrity.

Framework Evaluation

This paper isn't meant to steer organizations in one direction or another, but rather to give light to the factors that all organizations should be considering when selecting a risk management framework. That said, the table below presents a single-pane-of-glass view into some of the more common and accepted risk management frameworks and how they relate to the topics discusses in this paper.

It is also important to remember that while framework evaluation is often the most time-consuming first step on the path to achieving risk management objectives, it is only the tip of the iceberg. Organizations must reach a consensus on how to align threats to security controls, measure the effectiveness of implementation, report on progress to stakeholders, demonstrate compliance, negotiate control responsibilities with service providers, address third-party risk management and much more.

Organization/ Framework	HITRUST (CSF)	ISO (27001)	NIST (800-53 r5)	PCI (DSS v4.0)	AICPA (SOC 2 Type II)	HHS (HIPAA)
Transparency						
Authorship	HIGH	MED	MED	LOW	LOW	LOW
Agnosticism	HIGH	HIGH	HIGH	LOW	HIGH	LOW
Availability and Comprehension	HIGH	HIGH	HIGH	HIGH	HIGH	MED
Framework Precision	HIGH	MED	MED	LOW	LOW	LOW
Measurement & Accuracy	HIGH	MED	MED	LOW	LOW	LOW
Consistency						
Internal Effectiveness	HIGH	HIGH	HIGH	MED	MED	LOW
External Assessment	HIGH	HIGH	MED	MED	MED	LOW
Supply Chain Acceptance	HIGH	HIGH	HIGH	HIGH	HIGH	MED
Integrity	HIGH	MED	LOW	MED	MED	LOW

Conclusion

An assessment report is only useful or reliable if the level of assurance it provides is appropriate for the intended purpose. It is crucial that organizations undergoing an assessment understand the intended use for the assessment report, whether it be for internal management, a Board of Directors, customers or others. When it comes to vendors, organizations must also understand the level of assurance that is being provided as part of third-party risk management efforts. Remember to always consider the factors covered throughout this paper: transparency, accuracy, consistency and integrity. Embracing these principles in your approach should pay returns for your information security and risk management programs.

About the Author

Andrew Hicks is the National HITRUST Practice Leader and Vice President of Risk Assurance for Frazier & Deeter. He specializes in working with organizations to adopt, implement and manage information security programs, specifically in regards to HITRUST, HIPAA regulatory compliance, risk management and SOC examination procedures. A frequent speaker at HITRUST events, Andrew has managed more than 500 HITRUST engagements and has been repeatedly appointed to HITRUST Assessor, Quality and Marketing councils.

Find more information about Frazier & Deeter's HITRUST services here.