NIST
Cybersecurity Framework Success Story
ISACA

The voluntary Framework for Improving Critical Infrastructure Cybersecurity was developed through a collaborative process by industry, academia, and government stakeholders. It enables organizations – regardless of size, sector, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience. NIST does not validate or endorse any individual organization or its approach to using the Cybersecurity Framework.

Benefits from Using the Framework:

- The Cybersecurity Framework has **helped ISACA to provide the "so what" when conveying the importance of cybersecurity** to its 140,000 constituents around the globe. The Framework reinforces the relevance of the field and solidifies understanding of cybersecurity's importance to organizations' missions.
- Connecting ISACA's cybersecurity training to the Cybersecurity Framework has **provided a guidepost for training development** for individuals at all phases of their career journey, from the newest initiate to the battle-hardened incident responder.
- The Framework **provides a common ground in cybersecurity discussions**. Using the shared vernacular ensures that a common understanding is at the root of ISACA's cybersecurity programs and developments.

Situation

- As a worldwide non-profit association, ISACA engages in the development, adoption, and use of globally applicable, industry-leading knowledge and practices.
- ISACA was incorporated in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the growing field of auditing controls for computer systems. Today, ISACA serves 140,000 professionals in 180 countries.
- ISACA provides practical guidance, benchmarks, and tools for enterprises that use information systems. Through its comprehensive publications and services, ISACA defines roles for information system governance, security, audit, and assurance professionals worldwide.

Drivers

ISACA leverages multiple frameworks in development of its offerings. The Cybersecurity Framework has provided ISACA with a cornerstone to build its training and certification offerings around due to its ability to distill important elements among many available references. By leveraging the Framework, one can quickly identify the relevance of an effort, the domain in which it takes place, and the supporting national and international models and policies.

"The value of the NIST Cybersecurity Framework cannot be overstated for our organization, as the Framework has provided a common language to organize and communicate about our events, cybersecurity certifications, and training offerings."

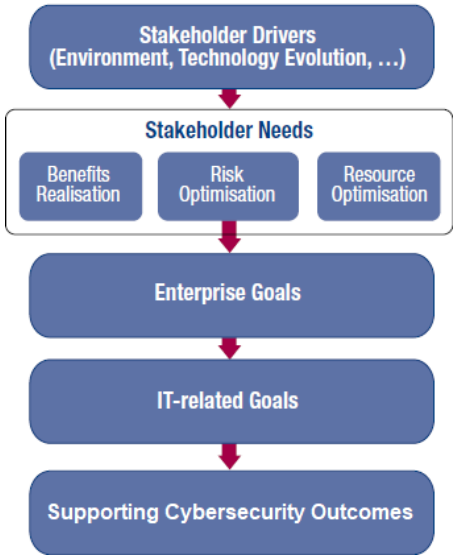
– Frank Downs, Director of Cybersecurity Practices, ISACA

Process

- To help foster awareness and improvement of the Framework, ISACA has presented during Framework workshop sessions, provided feedback on the Framework, and conducted surveys on the Framework's use. Through a survey of numerous CISOs and those who hold the Certified in Information Security Management® (CISM®) certification, ISACA found that of the nearly 800 respondents, over 75% were aware of the Framework and believed it helps to elevate the overall importance of cybersecurity.
- ISACA also integrated the Cybersecurity Framework's *Steps for Establishing or Improving a Cybersecurity Program* with its own COBIT model to help enterprises achieve objectives for the governance and management of enterprise IT. The published guide, and the associated course and certification examination, have been highly successful and have helped thousands gain the benefits of applying the Cybersecurity Framework.
- Leveraging the Cybersecurity Framework helps align ISACA's international training and certification products with key policies within the cybersecurity arena. The subcategory informative references point trainees and certification candidates to important policy points which define the cybersecurity field.
- ISACA members have benefited from numerous templates, tools, and webinars demonstrating effective tips and methods to apply the Cybersecurity Framework. Several of these resources are available on the NIST Cybersecurity Framework Resources pages.

Process (cont.)

- While the Cybersecurity Framework is not posed as a standard, ISACA uses elements (e.g., the Framework Core, Figure 2 regarding organizational information and decision flows, Implementation Tiers) to provide members with tools to help organize and conduct audit planning, activities, and reporting.
- ISACA has used the high-level functions of the Cybersecurity Framework to organize how cybersecurity topics are presented at events. For example, each of the sessions at the ISACA Cybersecurity Nexus (CSX) conferences is organized into Identify, Protect, Detect, Respond, and Recover tracks.



COBIT 5 Goals Cascade Supported by the Framework

ISACA Framework Implementation Overview

The Cybersecurity Framework is referenced in every cybersecurity training and certification product offered through ISACA. It is used to guide creation of each offering ranging from introductory courses explaining network communications to advanced certification exams that require extensive hands-on interactions with real cybersecurity incidents.

Results and Impacts

Integration of the Cybersecurity Framework into ISACA products has directly contributed to the international success of its cybersecurity products and has been specifically identified as a key element encouraging adoption of those products by individuals and enterprises.

Cybersecurity Framework integration has also been identified by ISACA constituents as providing relevance to all cybersecurity training and certification products – making them a default point of reference in training and career development.

By leveraging the Framework in its product development, ISACA has learned that many in the cybersecurity field desire training that connects good security practices with the business drivers behind them. Previously, some training and certification providers have relied on a hodgepodge of policies which abstractly connected to certain training elements. However, the Framework has improved guidance to trainees and certification candidates and has acted as the "go-to" reference for many in the field of cybersecurity.

What's Next

ISACA will continue to integrate the Cybersecurity Framework into its cybersecurity products and services. By implementing the Framework as its main cybersecurity guidepost, ISACA will continue to develop and deliver relevant professionalization products.

Contact Information & Resources

ISACA website: https://www.isaca.org/

ISACA Contact: Kristen Kessinger, communications@isaca.org

Cybersecurity Framework website: https://www.nist.gov/cyberframework

NIST contact: cyberframework@nist.gov