The Framework for Improving Critical Infrastructure Cybersecurity, published and maintained by the National Institute of Standards and Technology (NIST), enables organizations to apply ‘business drivers to guide cybersecurity activities’, ‘consider cybersecurity risks as part of the organization’s risk management processes’, and ‘align cybersecurity activities with business requirements, risk tolerances, and resources.’ By applying the Cybersecurity Framework (CSF), an organization can profile current cybersecurity risk and define a target state that best aligns with its unique risk tolerance.

The CSF can be applied to capture an organization’s Current Profile and Target Profile as part of their Risk Management Process. Those profiles can in turn be used to define gaps, prioritize operations, and to measure and assess progress - always in relation to business objectives.

**How is IACD related to the Cybersecurity Framework?**

IACD provides a mechanism where business- and operations-driven objectives, processes, and controls – including those captured via a CSF profile – can be translated and applied as automated response actions. Via *IACD Playbooks*, conditions, indicators and controls driving a cybersecurity response are captured, and orchestration services monitor and execute those playbooks.

An organization can apply the CSF without IACD capabilities or apply IACD capabilities without tying it to a CSF Target Profile. However, the employment of IACD playbooks provides organizations an opportunity to harness their technical security solutions to implement cybersecurity operations that align to their targeted risk profiles.

There is immediate benefit to the more mature organizations who have resources to apply to on-going cybersecurity management, but the ability to translate risk-derived priorities into actionable playbooks also benefits smaller or less-resourced organizations, perhaps even allowing them to leapfrog CSF tiers.
• **Cyber Operations Planning, Training, and Management:** IACD playbooks can be used to capture - in a consistent manner - procedures for key events and incidents *even if little or no automation is immediately enabled*. They become a knowledge base of operational and business rules driven by your risk profile. They can be distributed across locations and modified according to local policies, but maintain consistent traceability to the risk-derived priorities established by the organization. Changes in procedures or policy can be disseminated more effectively, and automation can be gradually enabled without redesigning solutions.

• **Ability to leverage best practices:** Commonly understood templates for playbooks are already being developed across communities of trust, commercial solution providers and security integrators. These can be used to more rapidly derive tangible benefits and lower the cost of entry into more mature capabilities.

• **Built-in measurement opportunities:** IACD Playbooks can be tied to risk metrics and measures, and also automate the collection of measures. The frequency of playbooks triggering and their effectiveness when employed can be traced to reflect their utility to your operations.

• **Flexibility to adopt new, innovative approaches:** Abstracting operational flows into IACD playbooks allows you to consider different actions or new solutions without risking your existing cybersecurity investments. IACD’s plug-and-play architecture can allow portions of an enterprise to try different approaches, but tie them to the same business/operations-driven playbooks.

• **Potential for risk-sharing, cost-sharing, and coordinated operational response:** As communities document their best practices – and are able to abstract the *practice* from the *organization-specific technical implementation* – members can share playbooks, measures, and other
practices in a way that benefits the whole community. Organizations with more limited resources can share cost and risk by collaborating on playbook development and execution.

**What’s next?**

The cybersecurity industry and community has the opportunity to develop, share, and collaborate on common playbook templates that trace to actions and controls that enable cybersecurity risk management. Orchestration solution vendors, service providers, and operations representatives are invited to participate in creating common specifications for security automation playbooks. For more information, go to: [https://secwww.jhuapl.edu/iacdcommunityday](https://secwww.jhuapl.edu/iacdcommunityday) or email iacd@jhuapl.edu.