Demonstrating Secure, Auditable, & Responsible AI

As AI systems grow in proliferation and impact, users and customers of business leveraging AI capabilities are demanding evidence their AI systems are secure, transparent, and aligned with relevant regulations. AI system certification attesting trustworthiness, accountability, and compliance is critical to gain market confidence. This is especially true in healthcare, finance, and other regulated industries.

The AI trust landscape can be daunting due to the disparate standards and principles. HITRUST has been an organization that has mapped various standards including NIST, ISO/IEC, and HIPPA into a single manageable Common Security Framework (CSF). It has recently released AI Security and Risk Management Framework to help organizations assess and demonstrate AI maturity. Below are key points useful for organizations interested in gaining HITRUST certification to increase market confidence in their AI practices and capabilities:

1. AI-Specific Controls: HITRUST released 90 new controls in its latest AI Security and Risk management framework. They are grouped into information protection, access control, risk management, training & awareness etc. To effectively respond to the requirements and manage interdependency, it is important to manage the controls by these domain groupings.

2. Control Evidence: Organizations must demonstrate control in three levels: Policy, Procedure and Implementation. Policy focuses on the control objectives given the organization context. Procedure outlines the operational steps to achieve the objectives. Implementation demonstrates the policies & procedures are practised operationally.

3. Existing Standards & Controls: Many of the AI controls can be satisfied with enhancements to existing controls given a mature IT practice. E.g., requirement for AI Asset Management (e.g., AI systems, model cards, and data) should be incorporated into existing IT asset management. Similarly, existing controls addressing IT risk management, access control, and data & privacy protection should and can be incrementally expanded to meet AI needs.

4. Evidence Repository: It is critical to establish an evidence repository to track and share the policy, procedure, & implementation evidence. This will serve as the authoritative source of truth in the final certification audit.

5. Early Version: It would not be controversial to suggest the current HITRUST AI controls represent a good ‘version one’ but improvements are expected. Increased requirement clarity, succinctness, and control coordination will improve the overall effectiveness. However, organizations should not hesitate to engage as this baseline version offers a good starting point.

At **www.previsant.com** we are proud to support organizations as they lead with secure, auditable, and responsible AI.

Brian Ng, Founding Partner Previsant Insights
brian.ng@previsant.com