Cybersecurity, Digital Assurance, and Compliance for System Integrators: PEGA

Under Development

This page is under development.

Practices and processes aimed at ensuring the security, reliability, and regulatory adherence of software systems. Integrating security measures, conducting vulnerability assessments, performing penetration testing, and ensuring that software deployments adhere to industry regulations and compliance standards.

Table of Contents

Additional Resources

https://www.pega.com/trust

More... Less...

Minor ATO Process

DTC's Pega environment holds a moderate Authority to Operate (ATO) at the platform level with high authorization anticipated July 2024. Every new application being built on the DTC's environment that is categorized as a minor application will require an Assess Only Approval and must be associated to DTCs Pega Cloud for Government Platform.

Minor ATO TIMLINE: 12 weeks from completion of intake

Minor ATO Tasks	High Level Steps & Responsibility
Task 1: Discovery / Requirements Validation	1.After product request (PR) is received and begins working through the Intake/Triage process, Cybersecurity is notified of the PR. 2.Intake team initiates Privacy Threshold Analysis (PTA) **Business Owner Input:** *BO should be prepared to provide any requested information from the intake team around data elements, use case & review PTA.* 3.Supplemental Security Questionnaire is provided to the Business Owner (BO), Development team, and SI's (System Integrators) **Business Owner & SI Input:** *BO & SI should be prepared to complete Supplemental Security Questionnaire.* 4. Data Security Categorization (DSC) is initiated **Business Owner Input:** *BO should be prepared to provide data elements for their use case.*
Task 2: Security Assessment Review Meeting/Call	1.DTC Product Stream Lead (PSL) will schedule Security Assessment Review Meeting **Business Owner Input:** *BO should be prepared to attend the Security Assessment Call and be prepared to speak to the data elements, use case & impact should the data be lost or compromised* 2. Continued finalization of PTA **Business Owner Input:** *BO should be prepared to collaborate on PTA completion with DTC intake*
Task 3: Completion of Data Security Categorization (DSC)	1. After the Security Assessment Call, VA Cloud Security will complete DSC and route for signature. **Business Owner Input:** *BO should be prepared to review and sign the completed DSC* 2. Continued finalization of PTA & determine if PIA is needed **Business Owner Input:** *BO should be prepared to collaborate on PTA completion with DTC intake*

Task 4: ATO Registration	1.Cybersecurity System Steward initiates ATO Registration
Task 5: Register Package in eMASS	1.Cybersecurity System Steward creates the ATO package with eMASS entry
Task 6: Security Assessment - RMF Process	**Low/Moderate Impact Packages:** 1.Cybersecurity System Steward completes necessary RMF steps within eMASS to complete the minor ATO 2. Cybersecurity System Steward submits the finished package to ISSO, followed by ISO for review 3. AO determines authorized termination date (ATD), the date at which renewal is required **High Impact Packages:** 1.Cybersecurity System Steward completes necessary RMF steps within eMASS to complete the minor ATO 2. Cybersecurity System Steward submits the finished package to ISSO, followed by ISO for review 3. Package is submitted to AOSB for final approval prior to the ATO briefing 4. ATO briefing held and package is approved with AO determined authorized termination date
Task 7: Package Moved into Continuous Monitoring	1. After path of final approval, package moves into continuous monitoring and is monitored by DTC Cybersecurity System Stewards 2. DTC Cybersecurity System Steward ensures package is ready for renewal ahead of ATD date **Business Owner & SI Input:** *BO's & SIs should be prepared to collaborate on the yearly PTA/PIA updates*

Minor ATO Process FAQs

Question	**Answer**
What is a PTA?	**Privacy Threshold Analysis (PTA):** A PTA is used to identify IT systems, rulemakings, programs, or pilot projects that involve SPI and other activities that otherwise impact the privacy of individuals as determined by the Director, Privacy Service, and to assess whether there is a need for a PIA, whether a System of Records Notice is required, and if any other privacy requirements apply to the IT system. A PTA includes a general description of the IT system, technology, rulemaking, program, pilot project, or other Department activity and describes what SPI is collected (and from whom) and how that information is used.
What is a PIA?	**Privacy Impact Assessment (PIA):** If the PTA of a system identifies the use or access of PII/PHI, then a PIA must be completed. PIA is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

What is an MOU/ISA?	**Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA):** A document established between two or more parties to define their respective responsibilities in accomplishing a goal or mission. an MOU or MOA defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. **Interconnection Security Agreement (ISA):** An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) between the organizations.
What is BAA?	**Business Associate Agreement (BAA):** A Covered Entity under HIPAA is a health plan, certain healthcare providers, or a healthcare clearinghouse. A Covered Entity must enter into a BAA with any person or organization that requires access to the Covered Entity's protected health information (PHI) in order to perform certain payment or health care operations activities or functions on behalf of the Covered Entity, or to provide one or more of the services specified in the Privacy Rule to or for the Covered Entity. When these payment or health care operations activities, functions or services are performed by a Business Associate on behalf of a Covered Entity, a BAA is required even in situations when there is no underlying contract or other agreement between the Covered Entity and the Business Associate.

Sec Risk Process- *COMING SOON!*