P.05 Indiana RAMP Policy for Cloud Offerings

P.05

Policy Name

Indiana Risk and Authorization Management Program (RAMP) Policy for Cloud Offerings

1. Purpose

Risk and authorization management programs – or "RAMPs" – are intended to protect data and technology resources while making the process of contracting for cloud offerings more straightforward, predictable, objective, and uniform. They achieve this by setting basic requirements for security assessments, authorizations, continuous monitoring, and other necessary components of cloud contracts that cloud providers are expected to meet. The requirements are based on generally accepted industry standards and are established in the form of minimum security-level matrices with different security controls that are based on the data and infrastructure involved and the impact of their potential loss or disruption. FedRAMP, the federal government's RAMP, is one example. The purpose of this policy is to create a RAMP for the State of Indiana.

2. Scope

This policy applies to all executive branch state agencies, departments, institutions, and similar entities that are responsible to the Governor of the State of Indiana. It also applies to any other entities that utilize, integrate with, or are otherwise connected to the State's systems, network, or other IT infrastructure. All such entities are covered by the scope of this policy, and all such "covered entities" must abide by its requirements – for any contracts for cloud offerings which are executed, amended, or renewed on or after October 14, 2025 – because of our collective need to protect data and the technology resources that are used to store, process, and transmit it.

3. Policy

3.1 Definitions

a. "Cloud offerings" are on-demand software applications, virtualized computing hardware (such as servers, storage, networks, and other infrastructure), or entire platforms for managing these resources that are provided over the internet. These products are frequently sold as "subscriptions." In such cases, they are commonly referred to as "software as a service," "infrastructure as a service," "platform as a service," and the like. They may also be included as part of a service that is provided by a vendor – for example, when an agency procures commercial off-the-shelf offerings from a third-party reseller or uses a vendor to develop and build systems outside of IOT's data centers and tenants. In most cases, the use of cloud offerings results in data being maintained remotely on servers, in data centers, or on other infrastructure that is not located within a state-owned datacenter or IOT-managed infrastructure or cloud tenants.
b. "Covered entities" are executive branch state agencies, departments, institutions, and similar entities that are responsible to the Governor of the State of Indiana as well as any other entities that utilize or are otherwise connected to the State of Indiana's systems, network, and other IT infrastructure.
c. "Critical infrastructure," for the purposes of this policy, refers to the systems and assets that are vital for society's smooth and safe operation. They are resources that Hoosiers depend on daily, in one way or another. Some tangible, physical examples are roads, bridges, power plants, electrical grids, water treatment plants, communication networks, transportation networks, hospitals, banks, and essential government facilities. Some intangible, virtual examples are the internet and essential government services. Disruption to critical infrastructure can have severe consequences on society's economy, security, health, and general well-being.
d. "IOT" means the Indiana Office of Technology, the executive branch agency of the State of Indiana created by IC 4-13.1, or its designee.
e. "Maturity assessor" means an independent, nationally recognized, compliance authorization organization with multistate connections.
f. "Minimum security level matrices" are the two-part framework to be used for selecting the minimum verified security designation levels - also referred to as GovRAMP statuses - that are required for cloud offerings, based on the data and infrastructure involved and the impact of their potential loss or disruption. There are three different levels in the matrices: GovRAMP Core, GovRAMP Authorized, and GovRAMP Authorized + CJIS Overlay. Each level calls for different NIST 800-53 controls to be in place. The minimum security level matrices are available, below, in Appendix 1.

3.2 Requirements

a. Cloud offerings must not be procured, otherwise obtained, or used unless they have been approved by IOT.
b. Proposed solicitations for cloud offerings must be provided to IOT no less than 90 days prior to the anticipated release to potential cloud providers for bidding, so that they can be meaningfully reviewed and approved.
c. Cloud offerings must:
    i. Comply with the NIST 800-53 controls that are necessary to meet the minimum security designation levels, which are called for by the minimum security level matrices in Appendix 1, by a reasonable date certain from the date on which they are procured, otherwise obtained, or used by a covered entity, not to exceed 18 months of the effective date of the resulting contract or one-half its term, whichever is shorter;
    ii. Continue to meet the necessary levels throughout the term of the contract, as determined by a maturity assessor, with evidence of the same being provided to covered entities and IOT on no less than a quarterly basis; and
    iii. Have regular risk assessments and continuous monitoring conducted on them, by a maturity assessor, throughout the term of the contract.
d. Contracts for cloud offerings must include language by which cloud providers agree to the requirements of Section 3.2.c, above.

4. Exceptions

The requirements of this policy are the default standards for 100+ state agencies, departments, institutions, and similar entities that are responsible to the Governor of the State of Indiana, as well as any other entities that utilize the State's systems, network, or other IT infrastructure. They are intended to protect the data of these different entities and the technology resources that are used to store, process, and transmit it. The minimum security level matrices that are discussed in this policy are based on generally accepted industry standards that cloud providers should be familiar with and amenable to.

In the rare case when a covered entity believes that an exception to the requirements of this policy are warranted for a particular contract that it wishes to enter into, the covered entity should be prepared to describe the cloud offering in question, how it will enable the covered entity to serve Hoosiers, how much it costs, and whether sensitive data and/or critical infrastructure is involved and the volume thereof. The covered entity should also be prepared to describe precisely how the requirements should be modified and why it believes the modifications are warranted under the circumstances, because it has concluded that the security risks associated with making them are outweighed by the benefits to the covered entity's business and mission. Lastly, before an exception request is submitted to IOT, it must be approved by the highest-ranking authority at the covered entity (executive director, commissioner, agency head, etc.), who must acknowledge that he or she has reviewed the modifications and believes 4 an exception is warranted because the benefits to the covered entity's business and mission are judged to outweigh any associated security risks.

Exception requests must be submitted by means of IOT's electronic form, which is available via request at IOTContractExceptions@iot.in.gov.

5. Ultimate Authority

Executive Order 25-19 specifically directs IOT to create a RAMP policy like this one for the State of Indiana. IOT is also statutorily authorized by IC 4-13.1-2-1 and -2 to establish technology and cybersecurity policies for the State.

6. Roles and Responsibilities

a. The role of covered entities, regarding the cloud offerings that are discussed in this policy, is to act as the frontline protector of data and the technology resources that are used to store, process, and transmit it. Specifically, covered entities are responsible for:
    i. Ensuring that they do not procure, otherwise obtain, or use cloud offerings that have not been approved by IOT;
    ii. Providing solicitations for cloud offerings to IOT, no less than 90 days prior to the anticipated date of release, so that they can be meaningfully reviewed and approved prior to release;
    iii. Identifying and selecting the minimum security designation levels for cloud offerings that are called for in the minimum security level matrices in Appendix 1;
    iv. Including language in their contracts calling for their cloud providers to agree to the requirements of Section 3.2.c, above; and
    v. Receiving and reviewing evidence that their cloud offerings continue to meet minimum security designation levels on no less than a quarterly basis throughout the term of the contract; notifying IOT via email to IndianaRAMP@iot.in.gov that their cloud offerings no longer meet minimum levels when applicable and within 30

days of learning of the same; and conferring with cloud providers to determine whether the failure to meet minimum levels can be resolved within timeframes that are acceptable to both the covered entities in question and IOT.

b. The role of IOT is to be a second-line evaluator of the decisions that covered entities make with regard to cloud offerings and the contracts that they desire to enter into with cloud providers. Specifically, IOT is responsible for:
    i. Reviewing solicitations for cloud offerings that have been provided by covered entities;
    ii. Reviewing the minimum security designation levels that have been identified and selected by covered entities for cloud offerings and considering whether they are appropriate;
    iii. Reviewing contracts for cloud offerings to ensure that they include language calling for cloud providers to agree to the requirements of Section 4.c, above;
    iv. Receiving and reviewing email notices from covered entities regarding the failure of cloud offerings to continue to meet minimum levels, conferring with covered entities to determine whether the failure can be resolved within a timeframe that is acceptable to IOT, and informing the covered entities in question and the Indiana Department of Administration that contracts are to be terminated in those cases where the failure cannot be resolved within timeframes that are acceptable to IOT.

7. Statutory Purposes

This policy furthers the purposes identified in IC 4-13.1-2-1.

8. Industry Standards

The Statewide IT Policies and Standards are based on the following:

Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, U.S. National Institute of Standards and Technology, Special Publication 800-37 Rev. 2. https://csrc.nist.gov/pubs/sp/800/37/r2/final

Security and Privacy Controls for Information Systems and Organizations, U.S. National Institute of Standards and Technology, Special Publication 800-53 Rev. 5. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Critical Security Controls v.8.1, Center for Internet Security. https://www.cisecurity.org/controls

9. Federal Audit

The federal government audits the IT practices of several Entities. Where necessary, those Entities may create agency-specific policies to supplement the Statewide IT Policies and Standards. Those agencies include the Bureau of Motor Vehicles, Department of Child Services, Department of Revenue, Department of Workforce Development, Family and Social Services Administration, Indiana Office of Technology, and the Indiana State Police.

Appendix 1

RAMP Minimum Security Level Matrices: *Data Type and Critical Infrastructure*

This appendix contains the two security requirement level matrices that covered entities are to use to identify and select the minimum security level for their cloud offerings. Matrix 1 pertains to “data type.” It requires covered entities to consider what type of data will be processed, stored, or transmitted by their cloud offerings. Matrix 2 pertains to “critical infrastructure.” It requires covered entities to consider whether critical infrastructure is supported in any way by their cloud offerings. Covered entities need to use both matrices to ensure that they identify and select the appropriate minimum verified security designation level or “GovRAMP Status.”

To use Matrix 1, covered entities should first look at Column 1 and determine what “data type” will be processed, stored, or transmitted by the cloud offering. There are three rows in Matrix 1 which correspond with the three different types of data for the purposes of this determination. Column 2 lists a handful of examples of various laws, regulations, and security policies that may apply to the three types of data listed in Column 1. The examples are provided for illustrative purposes only, in order to give covered entities an idea of the types of regulatory authorities that may apply to their data. Other authorities may also apply, however, and covered entities are expected to be familiar with the various authorities that apply to their particular data. Column 3 contains the corresponding

data classification types discussed in Statewide IT Policy IOT-CS-SEC-102. It is included for internal cross-referencing purposes only. Lastly, covered entities should look to Column 4 to determine which minimum security designation level applies to their cloud offering based on the data type in play: GovRAMP Core (which is the most basic level for nonconfidential data), GovRAMP Authorized (which contains additional requirements that are necessary to protect confidential data), or GovRAMP Authorized + CJIS Overlay (which contains even more requirements which are to protect CJIS Data). Each of those three levels require different NIST 800-53 controls to be in place. Additional information on GovRAMP statuses and the controls required for authorization under them can be found at https://govramp.org/providers/

Matrix 1			
1 - Data Type	**2 - Compliance/Regulatory Requirement**	**3 - Data Sensitivity Classification (per IOT-CS-SEC-102)**	**4 - Minimum Verified Security Designation Level Required (i.e GovRAMP Status)**
Data that is not required to be kept confidential by law, by contract, for business reasons, or for any other reason	NONE	Nonconfidential *or* Confidential - Proprietary	GovRAMP Core at the Moderate Impact level
Data that includes PII, PHI, FTI, PCI Data, SSA Data, education records, unemployment records, any other information that is required to be kept confidential by law, by contract, for business reasons, or for any other reason	Indiana Code, IRS Pub 1075, HIPAA, PCI, DSS, CMS, FISMA, 20 CFR 603, FERPA, others as applicable	Confidential - Sensitive *or* Confidential - Proprietary	GovRAMP Authorized at the Moderate Impact level
CJIS Data	CJIS Security Policy	Confidential - Sensitive *or* Confidential - Proprietary	GovRAMP Authorized + CJIS Overlay at the Moderate Impact level

To use Matrix 2, covered entities need to consider whether their cloud offerings will be used to support or could otherwise affect "critical infrastructure." For the purposes of this policy, "critical infrastructure" refers to the systems and assets that are vital for society's smooth and safe operation. They are resources that Hoosiers depend on daily, in one way or another. Some tangible, physical examples are roads, bridges, power plants, electrical grids, water treatment plants, communication networks, transportation networks, hospitals, banks, and essential government facilities. Some intangible, virtual examples are internet and essential government services. Disruption to critical infrastructure can have severe consequences impacting society's economy, security, health, and general well-being.

Matrix 2	
Critical Infrastructure?	**Minimum Verified Security Designation Level Required**
No	GovRAMP Core at the Moderate Impact level
Yes	GovRAMP Authorized at the Moderate Impact level

When covered entities determine that a higher minimum verified security designation level is required under one of the matrices than the other, they must select the higher level for their contracts. For example, if a covered entity determines that GovRAMP Core is

required under Matrix 1 but GovRAMP Authorized is required under Matrix 2, it must select GovRAMP authorized. Covered entities are always free to select higher levels for cloud offerings than is required by the matrices if they believe it makes sense to do so.