Deloitte.

Information Security Continuous Monitoring (ISCM)

Department of Information Resources (DIR)

March 2019

Introduction to Information Security Continuous Monitoring (ISCM)

What?

Maintain ongoing security awareness, vulnerabilities, and threats to enable organizational risk management decisions:

- Collect information based on established metrics utilizing information readily available in part through implemented security controls
- Regular (and as often as needed) data analysis to manage risk as appropriate for each organizational tier

Guiding Principles

National Institute of Standards and Technology (NIST)

- Special Publication (SP) 800-137 ("Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations")
- Special Publication (SP) 800-37 ("Risk Management Framework") – core of ISCM
- Interagency Report (IR) 8011 ("Automation Support for Security Control Assessments")

Benefits

Enables data-driven control of organization's cybersecurity posture through

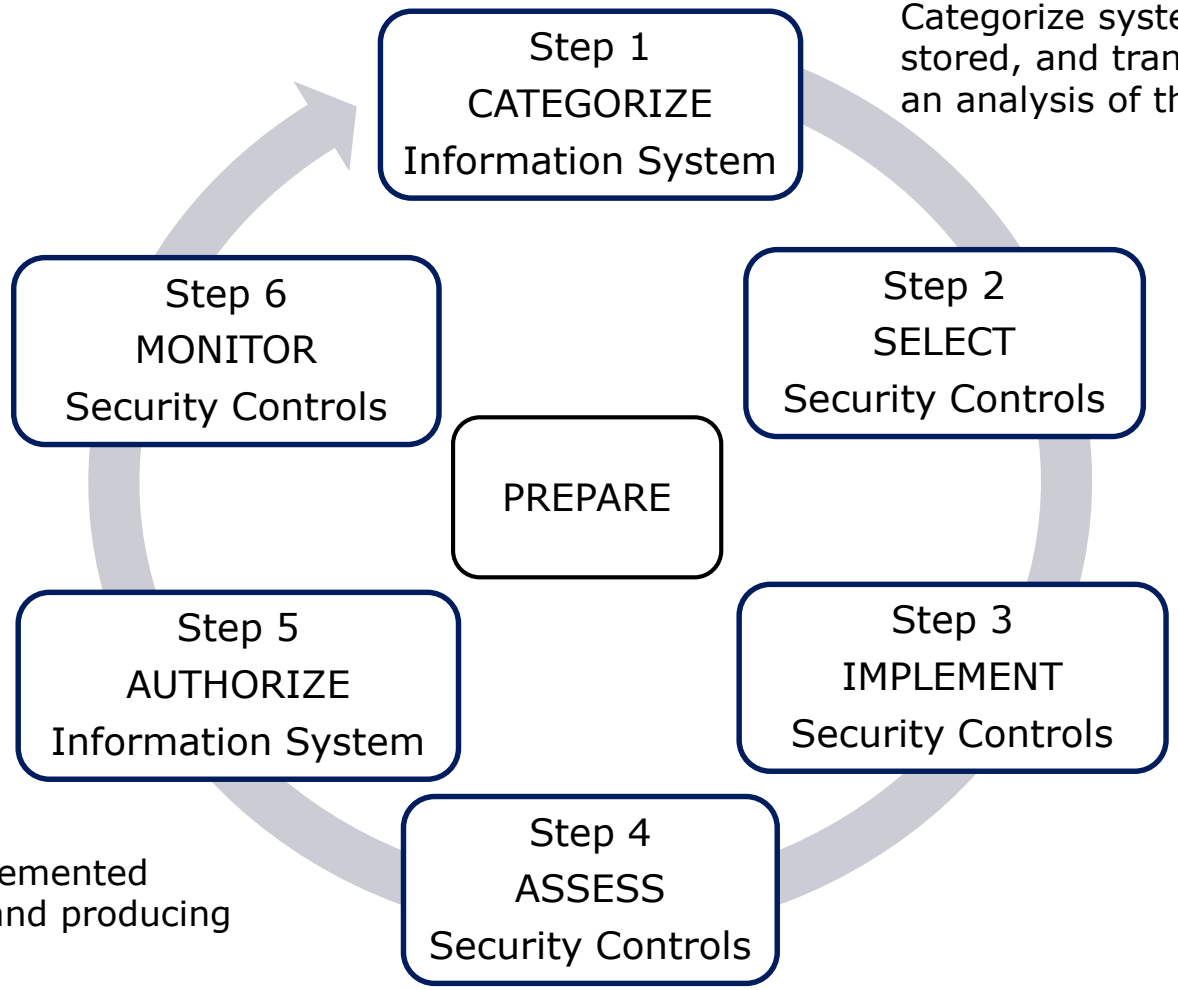
- Increased visibility into assets and awareness of vulnerabilities
- Improve and mature architectures, operational capabilities, and monitoring processes to accelerate response to threats and incidents
- Aligns to threat landscape and organization's priorities through periodic revision of ISCM strategy and program
- Prioritization of investments, resources and focus based on risk levels and posture
- Review and improve process efficiencies.

Texas Regulations

Texas Administrative Code (TAC) 202 and House Bill 4214 (Draft)

Source: National Institute of Standards and Technology

NIST Risk Management Framework – The Core of ISCM



Categorize system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss

Initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level

Enable controls and describe how the controls are employed within the system and its environment of operation

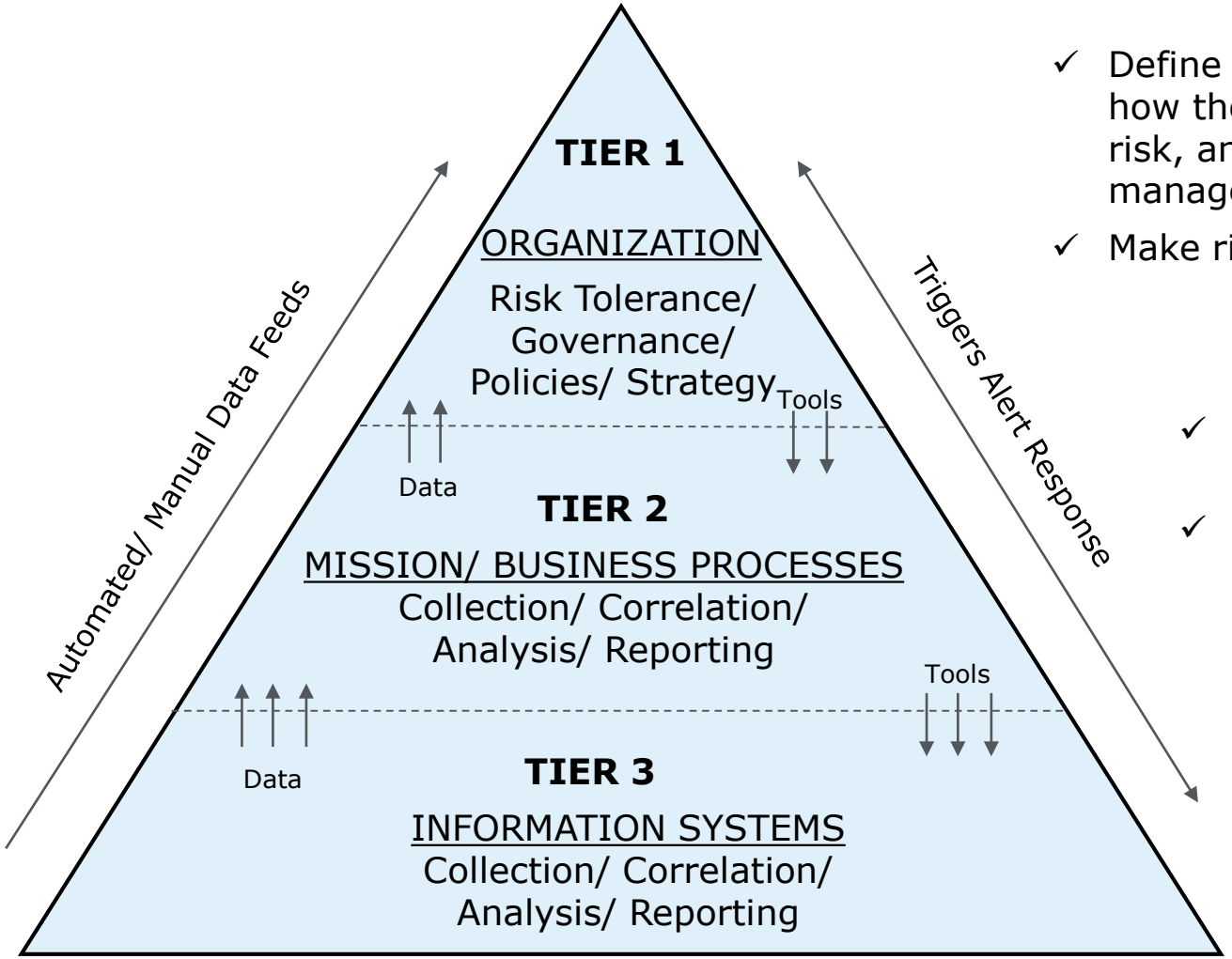
Determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes

Authorize system or common controls based on a determination that the risk is acceptable

Monitor system and the associated controls on an ongoing basis and reporting the security and privacy posture

Source: National Institute of Standards and Technology

Organization-Wide ISCM and Risk Management Approach



- ✓ Define the organization's risk management strategy, including how the organization plans to assess, respond to, and monitor risk, and the oversight required for an effective risk management strategy
- ✓ Make risk management decisions in support of governance.

- ✓ Prioritization of core mission/business processes with the overall goals and objectives
- ✓ Enable successful execution of the stated mission/business processes, and the organization-wide information security program strategy.

- ✓ Enable system-level security controls are implemented correctly and operate as intended
- ✓ Produce the desired outcome with respect to meeting the security requirements for the system, and continue to be effective over time

Source: National Institute of Standards and Technology

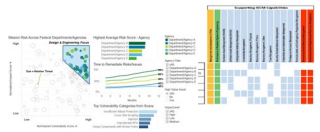
Building Blocks for ISCM Program

Agency Level Operational Dashboard and Reporting

Risk Scoring & Prioritization

Enterprise Level Operational Dashboard and Reporting

Legislative Reporting



Collection and Integration

Intelligence Sharing

Enterprise and other agencies

Integrated Collection and Aggregation

External sources

Intelligence Sharing

Foundation - Tools and Sensors

Assets

Devices

Network

Software

Cloud

Endpoints

Identity

Users & Access

Priv. Users

Network Security

Incident Response

Perimeter

Threat Intelligence

Patching

Event Mgmt

Defense in depth

Ongoing Authorization

Config. Mgmt

Data Protection

Endpoint protection

eDiscovery

Data Loss Prevention

Anti-Virus & Malware

Risk and Privacy

Vulnerability Scans

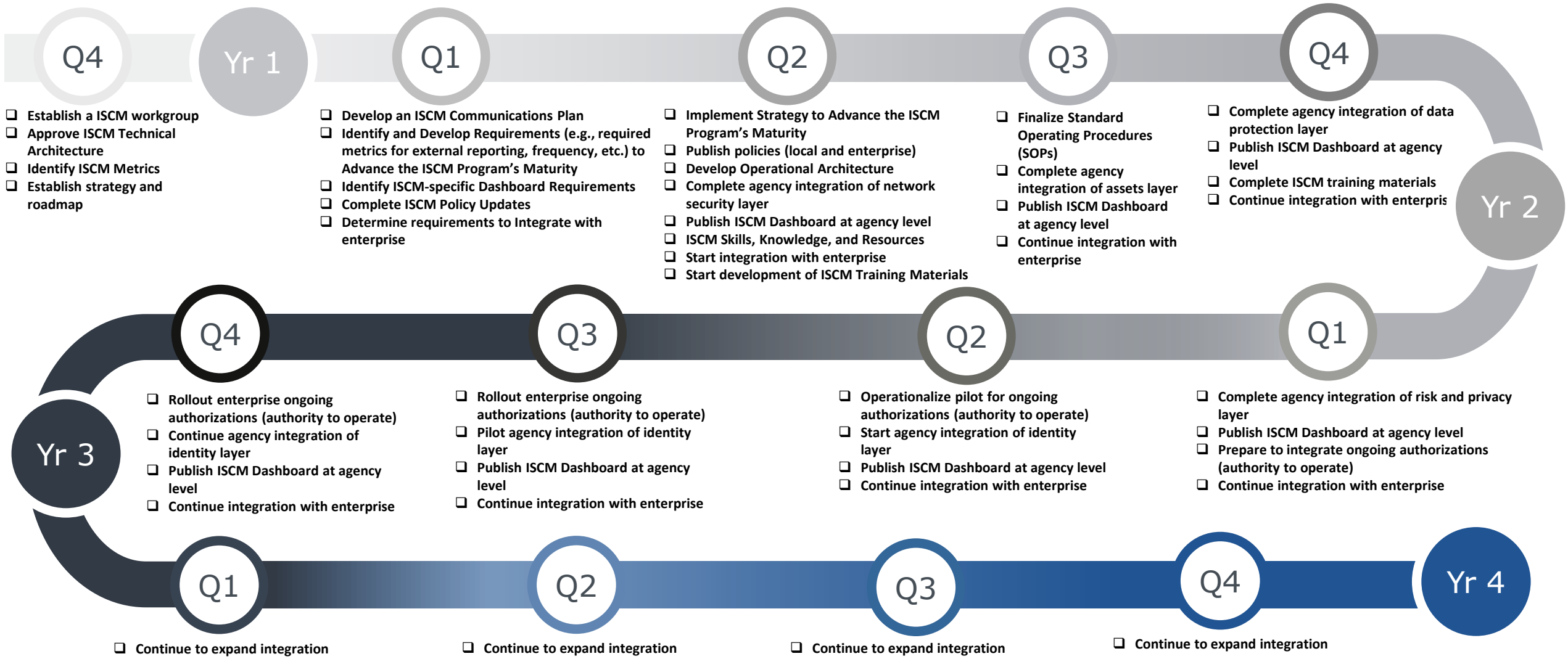
Data disclosure

Risk Register

Data breach

Source: National Institute of Standards and Technology, and Department of Homeland Security

Typical Roadmap



- ❑ Establish a ISCM workgroup
- ❑ Approve ISCM Technical Architecture
- ❑ Identify ISCM Metrics
- ❑ Establish strategy and roadmap

- ❑ Develop an ISCM Communications Plan
- ❑ Identify and Develop Requirements (e.g., required metrics for external reporting, frequency, etc.) to Advance the ISCM Program's Maturity
- ❑ Identify ISCM-specific Dashboard Requirements
- ❑ Complete ISCM Policy Updates
- ❑ Determine requirements to Integrate with enterprise

- ❑ Implement Strategy to Advance the ISCM Program's Maturity
- ❑ Publish policies (local and enterprise)
- ❑ Develop Operational Architecture
- ❑ Complete agency integration of network security layer
- ❑ Publish ISCM Dashboard at agency level
- ❑ ISCM Skills, Knowledge, and Resources
- ❑ Start integration with enterprise
- ❑ Start development of ISCM Training Materials

- ❑ Finalize Standard Operating Procedures (SOPs)
- ❑ Complete agency integration of assets layer
- ❑ Publish ISCM Dashboard at agency level
- ❑ Continue integration with enterprise

- ❑ Complete agency integration of data protection layer
- ❑ Publish ISCM Dashboard at agency level
- ❑ Complete ISCM training materials
- ❑ Continue integration with enterpris

- ❑ Complete agency integration of risk and privacy layer
- ❑ Publish ISCM Dashboard at agency level
- ❑ Prepare to integrate ongoing authorizations (authority to operate)
- ❑ Continue integration with enterprise

- ❑ Operationalize pilot for ongoing authorizations (authority to operate)
- ❑ Start agency integration of identity layer
- ❑ Publish ISCM Dashboard at agency level
- ❑ Continue integration with enterprise

- ❑ Rollout enterprise ongoing authorizations (authority to operate)
- ❑ Pilot agency integration of identity layer
- ❑ Publish ISCM Dashboard at agency level
- ❑ Continue integration with enterprise

- ❑ Rollout enterprise ongoing authorizations (authority to operate)
- ❑ Continue agency integration of identity layer
- ❑ Publish ISCM Dashboard at agency level
- ❑ Continue integration with enterprise

- ❑ Continue to expand integration

- ❑ Continue to expand integration

- ❑ Continue to expand integration

- ❑ Continue to expand integration

Expectations of House Bill 4214 (Draft) – Agency Role

(b) Each state agency shall:

(1) Develop and maintain an information security continuous monitoring program that:

A. Allows the agency to maintain ongoing awareness of the security and vulnerabilities of and threats to the agency's information resources

B. Provides a clear understanding of organizational risk and helps the agency set priorities and manage the risk consistently

C. Addresses how the agency conducts ongoing authorizations of information resources technologies and the environments in which those technologies operate, including the agency's use of common controls

D. Aligns with the continuous monitoring guidance, cybersecurity framework, and risk management framework published in NIST Special Publications 800-137 and 800-53

E. Addresses critical security controls, including hardware asset management, software asset management, configuration management, and vulnerability management

F. Requires the integration of cybersecurity products

(2) Establish a strategy and plan to implement a program for the agency

(3) To the extent practicable, establish information security continuous monitoring as an agency-wide solution and deploy enterprise information security continuous monitoring products and services

(4) Submit specified security-related information to the dashboard established under Subsection (c)(3)

(5) Evaluate and upgrade information resources technologies and deploy new products, including agency and component information security continuous monitoring dashboards, as necessary to support information security continuous monitoring and the need to submit security-related information requested by the department

(6) Require that external service providers hosting state information meet state information security requirements for information security continuous monitoring

(7) Ensure the agency has adequate staff with the necessary training to meet the objectives of the program

Expectations of House Bill 4214 (Draft) – DIR Role

(c) The department shall:

(1) oversee the implementation of this section by each state agency

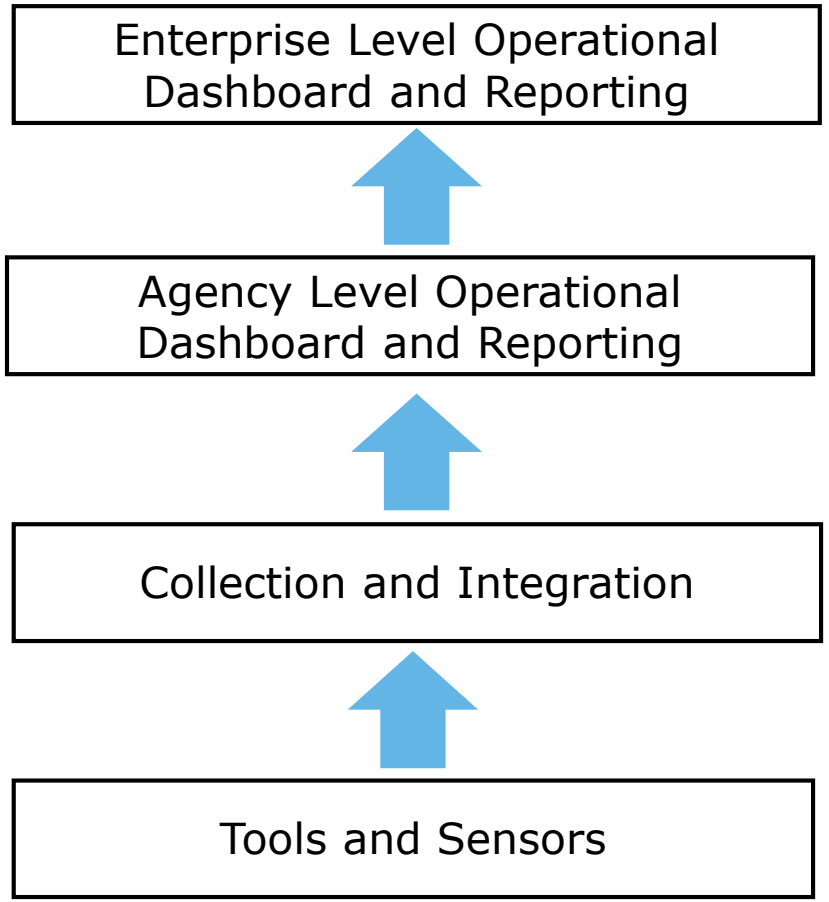
(2) monitor and assist each state agency in implementation of a program and related strategies

(3) establish a statewide dashboard for information security continuous monitoring that provides:

A. A government-wide view of information security continuous monitoring; and

B. technical specifications and guidance for state agencies on the requirements for submitting information for purposes of the dashboard.

Fiscal impact considerations



Key component for fiscal impact
- Business analytics tools
- Configuration, analysis and monitoring services

Key components for fiscal impact
- Log aggregators and SIEM
- Configuration, analysis and monitoring services

Key component for fiscal impact
- Tools and services not currently available to agencies

Example Dashboard

Please reach out to DIR Security for questions
dirsecurity@dir.texas.gov

Deloitte.