EXECUTIVE OFFICE OF TECHNOLOGY SERVICES & SECURITY

COMMONWEALTH OF MASSACHUSETTS | 1 ASHBURTON PLACE, 8TH FLOOR, BOSTON, MA 02108

**CHARLES D. BAKER**
Governor

**KARYN E. POLITO**
Lieutenant Governor

**Curtis M. Wood**
Secretary

January 27, 2020

The Honorable Suzanne Bump
State Auditor
State House, Room 230
Boston, MA 02133

Chair Aaron Michlewitz
House Committee on Ways and Means
State House, Room 243
Boston, MA 02133

Chair Danielle Gregoire
Joint Committee on State Administration and Regulatory Oversight
State House, Room 23
Boston, MA 02133

Chair Michael Rodrigues
Senate Committee on Ways and Means
State House, Room 212
Boston, MA 02133

Chair Marc Pacheco
Joint Committee on State Administration and Regulatory Oversight
State House, Room 312B
Boston, MA 02133

Dear Auditor Bump, Chair Michlewitz, Chair Rodrigues, Chair Gregoire, and Chair Pacheco:

Pursuant to Chapter 41 of the Acts of 2019, the Executive Office of Technology Services and Security (EOTSS) is pleased to provide you with the attached report detailing EOTSS' Information Governance Framework.

I am grateful for your continued partnership with EOTSS. Please feel free to contact Scott Ahern at Scott.m.ahern@mass.gov should you have any questions about this report.

Sincerely,

Curtis M. Wood
Secretary, Executive Office of Technology Services and Security

# Commonwealth of Massachusetts

## EOTSS Information Governance Framework

**Title:** EOTSS Information Governance Framework
**Creator:** Executive Office of Technology Services and Security
**Date Issued:** 12/31/2019

**Executive Office of Technology Services and Security**
*Our Mission: To provide secure and quality digital information, services, and tools to constituents and service providers when and where they need them.*

# Foreword from the Secretary

As required by the FY 2020 General Appropriations Act (GAA), EOTSS is charged with the creation and implementation of an "**Information Governance Framework" and Information Governance Program** which will provide independent planning, execution, and management of the necessary policies, standards, practices, technologies, and tools to support our information lifecycle, risk, and compliance needs at an enterprise level. This framework will serve to operationalize Information Governance (IG) in alignment with our capacities, capabilities, and legal requirements.

**EOTSS approaches Information Governance as a transformative, living program** that will, and should, evolve with our strategic goals, customer service needs, and lawful obligations. Its ultimate intent is to **promote a cohesive, enterprise-wide view of IG in order to build bridges across any existing gaps or silos**, enabling us to support the providers we serve and engage our constituents with increased efficiency, effectiveness, and transparency.

The EOTSS IG Program will highlight a few key functions that were specified within the budget, while also providing room for additional functions in the future:

- Defensible Destruction: Reduce the volume of data EOTSS manages to make information more easily located, accessible, and managed
- Information Lifecycle Management: Harmonize organization-wide policies and procedures regarding information – creating more efficient practices around use, retention, and disposal – and support functions such as E-Discovery, Cybersecurity, and data quality
- Staff On/Offboarding: Ensure employees understand EOTSS's IG needs and make IG more cohesive across the agency, facilitating more effective knowledge transfer and compliance/risk assurance
- Privacy and Security: Promote effective privacy and security controls so that EOTSS complies with requisite laws and standards, and proactively reduces the likelihood of incident events that would otherwise require time and resources to respond

This document then presents needs and goals across the following six areas that ultimately advance EOTSS's Information Governance efforts:

- Program Management: Provide IG management, oversight, and agency-wide direction around specific IG Functions, and establish a few key roles and responsibilities
- Strategic Planning and Implementation: Launch strategic principles and critical success factors to drive IG development and implementation
- Policy and Standards Development: Aggregate, organize, and coordinate existing EOTSS policies, while also creating new standards to comply with legal and regulatory requirements

- Communication and Training: Establish a central point of communication and training around IG, related compliance, and information management practices
- Metrics and Measurement: Aggregate, organize, and coordinate EOTSS's existing Key Performance Indicators (KPI's)
- Compliance and Risk Management: Provide independent IG compliance controls

Our IG Framework illustrates a commitment to governance by **setting in motion a series of planning and implementation efforts** to independently plan and operationalize IG policies and establish a "roadmap" for continued IG assessment and progress:

1. Launch the IG Program and internalize the IG Framework document
2. Establish a "Chief Compliance Officer" role, create an "IG Steering Group", and coordinate EOTSS's existing roles under the IG Program
3. Complete IG strategic implementation planning efforts
4. Continue to aggregate and coordinate information regarding existing IG-related efforts and information assets
5. Align compliance with MA guidelines and standards under the IG Program
6. Prioritize and process overall activities that support the launch of the IG Program and specific IG Functions
7. Advance IG through incremental phases and efforts

In addition to meeting the IG requirements established in the FY 2020 GAA, **EOTSS's goal is to realize sustainable and scalable information governance progress**. To do that, IG must be aligned firmly with the secretariat's strategic plans and objectives, legal requirements, and the ever-changing environment within which we operate. Most importantly, our IG efforts must support our staff, who ultimately carry out the mission and services of the Commonwealth of Massachusetts.

**EOTSS is collectively invested in the Commonwealth's and each other's success**. We aim to use our information resources to improve how we serve the Secretariats, agencies, and constituents of the Commonwealth. We aim to be a collaborative partner in working towards this goal.

**Curtis M. Wood**
Secretary, Executive Office of Technology Services and Security

# Table of Contents

# 1. Introduction

## 1.1 Purpose

The EOTSS Information Governance Framework (IG Framework) seeks to understand and address the Commonwealth of Massachusetts FY 2020 GAA[1] requirement to "*create and implement a comprehensive Information Governance Plan*." EOTSS has adopted the term "**Information Governance Framework**" to represent a holistic view of the interrelationships between various Information Governance (IG) components and provide a foundation from which ongoing IG efforts can be incrementally and iteratively completed.

## 1.2 Scope and Objectives

The IG Framework facilitates a logical distinction and linkage between IG program management, IG strategic planning, IG policy and standards development, the tactical implementation of IG, and ongoing monitoring and updates through the IG program. A key focus of this document is to establish the context that organizes the above, setting in motion the ongoing implementation of IG arranged under this framework.

## 1.3 Updates

As changes in legal requirements, information and data lifecycles, business needs, technologies, and policies occur, they should be assessed via the IG Framework to administer the impacts to EOTSS, its staff, its partners, and its constituents. With that in mind, updates to this document, as well as the specifications and policies that result from it, will be managed in accordance with guidance provided herein.

*[Remainder of this page intentionally left blank]*

[1] The 191st General Court of the Commonwealth of Massachusetts, FY 2020 GAA, 2019. Online at https://malegislature.gov/Budget/FY2020/FinalBudget

# 2. Background

## 2.1 Initiation of the EOTSS IG Framework

The formal basis for the development of the EOTSS IG Framework stems from the Commonwealth of Massachusetts FY 2020 GAA (FY 2020 Budget) language for EOTSS to "*create and implement a comprehensive information governance plan*."[2]

Recognizing that IG itself is not a "one size fits all" solution, EOTSS has adopted the perspective that IG advancement can be achieved via a coordinated, ongoing program centered around strategic planning, the development and operationalization of effective policies and standards, and continuous assessment. As such, EOTSS's IG Framework is an initial understanding of, and commitment to, this perspective and fulfilling the needs outlined in the FY 2020 Budget.

**EOTSS's IG efforts materialize its understanding of the "information governance plan" Budget language**

**EOTSS is launching its IG Framework to set an overall IG effort in motion**

**Inter-relationships of different IG components and IG Functions are organized under an "IG Framework"**

**The IG Framework establishes the direction for, and commitment to, ongoing IG efforts and progress**

**EOTSS will continue to make incremental progress under the direction of the IG Framework and IG Program**

*[Remainder of this page intentionally left blank]*

[2] The 191st General Court of the Commonwealth of Massachusetts, FY 2020 GAA, 2019. Online at https://malegislature.gov/Budget/FY2020/FinalBudget

## 2.2 The Need for IG

While the concept of "silos" is often used to describe information in isolated systems or applications, this term also applies to the select practices of IG by specific organizational units, job functions, and individuals. These practices could entail areas such as compliance with public records retention, the protection of personally identifiable information (PII), identifying when information is able to be destroyed or transferred, and dealing with information transition needs when staff are onboarding or offboarding.

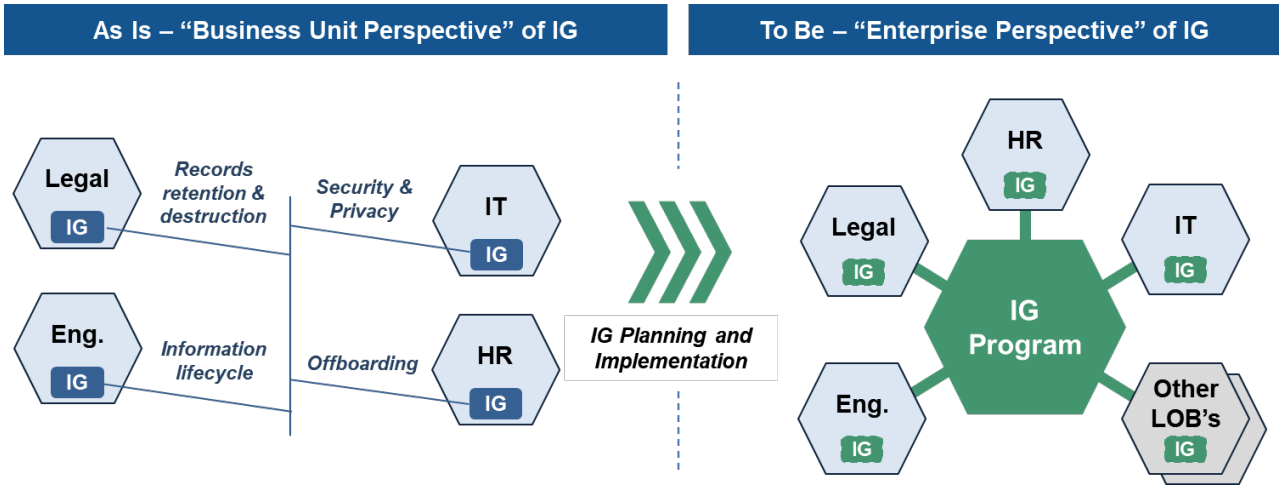



*Figure 1: Information Governance as a Transformative Process*

As illustrated in the above, IG-related policies, procedures, standards, and tools are often sourced from, and managed by, business units or lines of business (LOB's) with specific domain expertise in each area. This conventional practice is in alignment with the functions of an enterprise.

However, with the rapidly evolving environment of information management compliance, risk assurance, and value optimization, a "**siloed**" business unit perspective could present possible blind spots around achieving the best overall results for the enterprise. IG seeks to "**build bridges**" across these silos by promoting a cohesive, enterprise-wide view that:

- Organizes existing IG resources and efforts from business units
- Coordinates input and expertise from all business units
- Provides independent planning, implementation, and management of IG policies, procedures, tools, and training
- Establishes an evolving, sustainable, and scalable IG Program

## 2.3 Benefits of IG

By using IG as an over-arching strategy to organize, use, protect, and dispose of information in an efficient and accountable way, the Commonwealth will better serve its constituents and foster its effectiveness to:

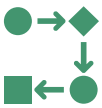
- Comply with **legal obligations** regarding transparency and accountability

- Ensure information **security** and **privacy**
- Identify opportunities to **optimize value** and **reduce costs**
- Create, use, retain, and **dispose of information efficiently**
- **Manage risk** associated with information assets
- Promote higher levels of **transparency** and **access** to **data**

These benefits can be seen "in action" throughout the day-to-day and big-picture activities of:

**Defensible Destruction**

By responsibly reducing the volume of data EOTSS manages, information will be easier to find, easier to access, and require less resources to store and/or manage



**Information Lifecycle Management**

By harmonizing organization-wide policies and procedures around when, where, and how EOTSS's information is used, more efficient practices around use, retention, and disposal can be implemented; and supporting functions such as E-Discovery, Cybersecurity, and data quality will be enhanced

**Staff On/Offboarding**

By ensuring employees understand EOTSS's IG needs, IG will be more cohesive across the agency, knowledge transfer during transitions will be more effective, and compliance/risk assurance can be fostered

**Privacy and Security**

By ensuring effective privacy and security controls, EOTSS will maintain compliance with the laws and standards EOTSS's is obligated to fulfill, and proactively reduce the likelihood of incident events that would otherwise require time and resources to respond

## 2.4 Coordination with Established IG-Related Areas

Records Custodians in the Commonwealth serve to fulfill several requirements and provisions established by the Supervisor of Records and Records Conservation Board under the Secretary of the Commonwealth of Massachusetts. Core responsibilities include, but are not limited to, compliance with:

- Public records law (PRR)
- Records retention schedules (RRS)
- Breach notification
- Protection of personally identifiable information (PII)
- Designation of a Records Access Officer (RAO)

- Designation of a liaison to the Records Conservation Board (RCB)
- Designation of a member of the RCB (where applicable)
- RCB transfer and destruction permissions
- EOTSS "Enterprise Information Security Standards"
- EOTSS Cybersecurity Readiness Framework

Additionally, in EOTSS's capacity as a technology service provider to other Commonwealth agencies, it is understood that EOTSS also serves as an "agent" of other record custodians through the hosting and physical care of records, however, "may not take action with respect to the records without the specific authority of the custodian."[3]

It is important to recognize these established areas when coordinating EOTSS's IG efforts, and also harmonization with, or updates to, the Commonwealth's "Electronic Records Management Guidelines"[3] jointly published by EOTSS (formerly the "Information Technology Division" (ITD) of the Executive Office of Administration and Finance) and the Secretary of the Commonwealth of Massachusetts.

*[Remainder of this page intentionally left blank]*

[3] Electronic Records Management Guidelines. Online at https://www.sec.state.ma.us/arc/arcpdf/Electronic_Records_Guidelines.pdf

# 3. Defining and Discerning IG

## 3.1 Approaching a Definition of Commonwealth IG

Information Governance is a multi-disciplinary framework "for managing information throughout its lifecycle and supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements."[4]

> **Practically speaking, IG can also be viewed as how easily information can be searched for, found, and produced in a cost-effective way that aligns with all information compliance and security requirements, strategic goals, and customer service needs.**

IG typically seeks to address the entirety of "information assets" for a given organization, which represents a significant need for coordination, governance, and ongoing support. Here, information assets are characterized as information (data) that an organization has assigned meaning or value through compliance or security requirements, business value, customer value, or otherwise.

EOTSS understands that successful IG is not a "one size fits all" solution, but rather, manifests itself in alignment with the unique needs, goals, risks, resources, and capabilities of a given organization. To that extent, IG seeks to harmonize all information management in alignment with an organization's:

- Strategic goals and objectives
- Roles and responsibilities
- Compliance requirements
- Risk, privacy, and security assurance needs
- Opportunities for adding value (or, reducing costs)
- Technical capabilities and capacity
- Existing IG-related policies, standards, procedures, and practices

## 3.2 Distinction of IG from its Sub-Domains

It is important to distinguish between IG and other, more granular sub-domains and concepts that operate under the umbrella of IG, including (but not limited to):

- IT Governance
- Data Governance
- Data Quality
- Metadata
- Master Data Management (MDM)

[4] AHIMA International's Information Governance FAQ. Online at https://www.ahima.org/topics/infogovernance/faqs?tabid=faq

- Records Information Management (RIM)
- Information Architecture
- Identity and Access Management (IAM)
- Information Security (InfoSec)

It is an implicit goal of the EOTSS IG Framework to incrementally and iteratively progress through IG concepts that support the needs of the agency; however, it is important to do so in a way that corresponds with EOTSS IG maturity, capacity, and capabilities. To that extent, EOTSS will evaluate and engage IG sub-domains accordingly. Please see the appendix of this document for high-level descriptions of each of the above.

*[Remainder of this page intentionally left blank]*

# 4. Strategic Principles and Success Factors

## 4.1 Strategic Principles

EOTSS's IG Program seeks to balance risk and investment related to the management of the information assets, while being unique to the Commonwealth's needs, capacity, capabilities, and compliance requirements. Continued growth and development of this effort is guided by the following strategic principles (IG-SP's):

| | |
|---|---|
| **IG-SP-1** | **Providing Staff with IG Guidance and Support**<br>Help the organization understand the value of effective, timely and consistent management of both physical and electronic information and educate personnel of their IG responsibilities to the Commonwealth. |
| **IG-SP-2** | **Complying with Legal Requirements and Commonwealth Transparency and Accountability Requirements**<br>Build upon EOTSS's existing work while also providing for more standardized and timely response to legal holds and governmental standards. |
| **IG-SP-3** | **Managing Risk**<br>Mitigate several risk factors, including but not limited to handling cybersecurity, identifying and indexing content that isn't readily accessible, understanding the balance of information retention vs. defensible destruction, and providing a clearer definition of "public record" for more nascent content types. |
| **IG-SP-4** | **Maintaining Information Security and Privacy**<br>Address various aspects of cybersecurity risks, information ownership, access control, and more focused elements of information privacy. |
| **IG-SP-5** | **Improving Information Lifecycle Efficiency and Value**<br>Establish further organizational efficiencies via the classification, consolidation and reduction of information assets. |
| **IG-SP-6** | **Realizing Cost Savings and Value Opportunities**<br>Save material expenses for the organization via IG, whether those costs are "hard," "soft," or "opportunistic" in nature. |

| | |
|---|---|
| **IG-SP-7** | **Serving EOTSS's Partners and Constituents**<br>Satisfy the needs of multiple players within the ecosystem via improvements in information access, availability, efficiency, engagement, and transparency. |

| | |
|---|---|
| **IG-SP-8** | **Enabling Proactive Decision Making**<br>Align divergent interests across various constituencies to agree on a decision-making framework that identifies future needs and the requisite strategic path. |

| | |
|---|---|
| **IG-SP-9** | **Ensuring all Tools and Technologies Map to Strategic Goals and Needs**<br>Leverage the IG framework to identify clear and tangible requirements for the evaluation, acceptance and usage of technologies. |

| | |
|---|---|
| **IG-SP-10** | **Aligning IG Program Goals with Enterprise Capacity, Capability, and Resources**<br>Match what EOTSS seeks from a fully functional IG program with the supporting assets, limitations, and timing within the organization. |

| | |
|---|---|
| **IG-SP-11** | **Continuously Updating the IG Program**<br>Evaluate the IG program, its components, and results on a continuous basis to understand what is working well and what changes are required in response to any unforeseen developments and requirements. |

## 4.2 Critical Success Factors

The Commonwealth is well versed in creating beneficial legal, regulatory, and policy-driven requirements for enterprises and agencies. However, the Commonwealth also has deep familiarity with the challenges of adopting, executing and supporting such requirements. These challenges are often heightened by the practical realities of enterprise resource constraints.

Various critical success factors impact the efficacy of EOTSS's IG Framework; however, it's ultimate success will depend on the following key factors:

### Maintaining Positive IG Culture and Executive Sponsorship

The IG Framework must address institutional challenges around change, willingness to engage, over-retention, and silo-based approaches to information management. Maintaining consistent executive sponsorship, leadership, and championing of IG that is "in touch" with the needs of the enterprise will be a central component to a positive culture around IG.

### Ensuring a Clear Understanding of IG Expectations and Requirements

The IG Framework must have three key aspects to meet expectations regarding EOTSS relationship with information:

- Satisfying information compliance requirements

- Managing information risks
- Optimizing information value

### Utilizing a Realistic IG Implementation Approach
The IG Framework must focus on confirming and advancing current maturity aspects in alignment with the capacity and capabilities of the enterprise.

### Providing Ongoing Communication and Support for IG
The IG Framework must create a holistic view of IG by creating effective communication and support programs to proactively engage all business units and staff.

### Leveraging Technology and Automation
The IG Framework must appropriately and strategically leverage technology to help automate IG where possible to mitigate risks around compliance, change, and culture.

### Ensuring Reasonable IG Compliance
Compliance with IG Framework policies, standards, or procedures must be reasonable and in-line with the capabilities and capacity of the enterprise. Effective, reasonable monitoring and compliance will incrementally eliminate “silos” of practices, inconsistent policies, and provide cross organizational implementation success.

### Risk Management
The IG Framework must align clearly with legal, privacy, security, and other risk-related requirements that impact the enterprise, and must ensure that no additional, unnecessary risk is unnecessarily introduced.

### Strategy and Planning
Deliberate strategic planning and related key performance indicators (KPI’s) should serve to proactively drive the IG Framework implementation efforts.

### Change Management
The IG Framework must continuously account for, and support, aspects of change management that address the cultural needs of the enterprise.

*[Remainder of this page intentionally left blank]*

# 5. IG Framework

EOTSS views effective IG as a living, evolving program with an "enterprise perspective" of the IG policies, standards, processes, tools, and measures across all information assets. While EOTSS's IG Framework seeks to describe the interrelationship between various IG components, the **IG Program** designates the continuous management of centralized IG independent from specific business units or areas.

As opposed to a one-time project, the IG Program is an ongoing effort to incrementally and iteratively advance IG. The continuous nature of the IG Program progressively develops IG while:

- Maintaining alignment with current capacity and capabilities
- Enabling adequate resource planning and funding
- Ensuring realistic and reasonable development
- Managing the impact of change
- Making ongoing assessment an implicit function

## 5.1 Centralized and Coordinated IG Program

EOTSS's IG Program provides a central governance body focused on achieving IG results, incorporating the input and needs of all business units, resolving potential IG conflicts, and integrating different aspects of IG established by the Secretary of the Commonwealth.

Centralized IG is largely most efficient as resources can be leveraged in a cost-effective manner and address enterprise-wide needs. This approach also offers reliable sustainability in the sense that the IG Program can exist independent of transition across the enterprise and provide uniform management of all IG needs with realistic autonomy.

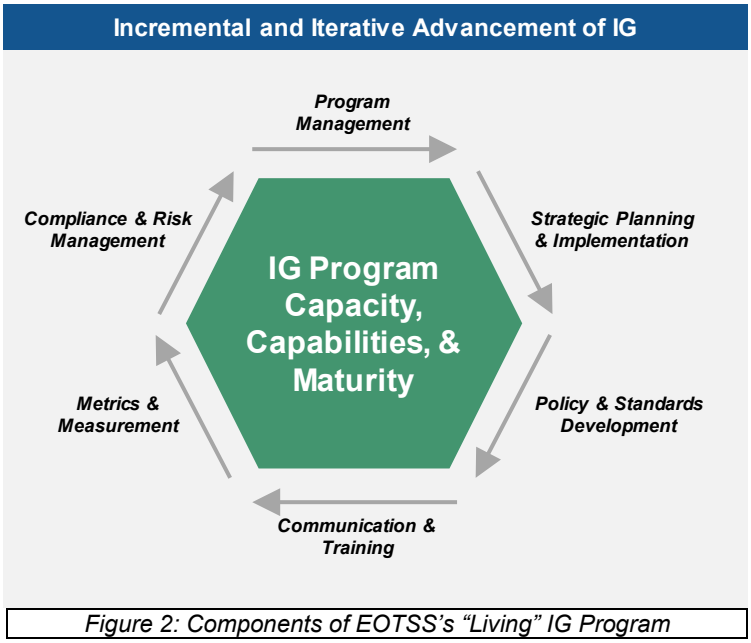



*Figure 2: Components of EOTSS's "Living" IG Program*

Establishing a sustainable, scalable IG Program is important when factoring in rapid changes across the information and technology landscape, as exemplified by dramatic increases in data generation and retention, hosting via third-party cloud providers, and evolving cybersecurity threats. Equally important is the continuous need to identify and realize opportunities around

organizational efficiency, cost savings, and meet the expectations of the Commonwealth and its constituents.

## 5.2 IG Program Components

As illustrated in Figure 2 ("Components of EOTSS's 'Living' IG Program") above, EOTSS's ongoing IG program can be characterized by the following interrelated components:

- Program Management
- Strategic Planning and Implementation
- Policy and Standards Development
- Communication and Training
- Metrics and Measurement
- Compliance and Risk Management

The following table describes each component in the context of the launch of EOTSS IG Framework and Program.

| IG Program Component | Description |
|---|---|
| **Program Management** | • Provides IG management, oversight, and agency-wide direction around specific IG Functions<br>• Establishes an EOTSS "Chief Compliance Officer" (CCO) for IG<br>  ○ Independent from all other EOTSS business units<br>  ○ Serves as the central IG compliance representative<br>  ○ Provides IG oversight and recommendations<br>  ○ Creates and works with new EOTSS IG Steering Group<br>• Establishes an EOTSS "IG Steering Group"<br>  ○ Coordinates existing EOTSS roles and responsibilities (Data Officer, Privacy Officer, Security Officer, etc.)<br>  ○ Interfaces with EOTSS business units<br>• Assesses and advances the "maturity" of EOTSS IG<br>• Continuously manages key IG risks, needs, and goals around information management |
| **Strategic Planning and Implementation** | • Establishes strategic principles and critical success factors to drive IG development and implementation<br>• Incorporates an agency-wide strategic view of IG<br>• Incrementally and iteratively develops an IG Strategic Implementation Plan and roadmap |

| IG Program Component | Description |
|---|---|
| | • Coordinates with EOTSS business units regarding specific IG-related policies, standards, procedures, projects, and tools<br>• Assigns resources to effectively manage and implement IG efforts<br>• Ensures all tools and technologies align with strategic principles and organizational goals |
| **Policy and Standards Development** | • Aggregates, organizes, and coordinates existing EOTSS policies and standards<br>• Evaluates policies and standards with an agency-wide perspective<br>• Creates new and adjusts existing policies and standards to:<br>  ○ Align and maximize value of resources agency-wide<br>  ○ Align with risks, needs, and goals<br>• Complies with legal and regulatory requirements (e.g., retention, privacy, etc.) |
| **Communication and Training** | • Establishes a central point of communication and training around IG, related compliance, and information management practices<br>• Aggregates, organizes, and coordinates EOTSS's existing IG communication and training efforts<br>• Supports understanding of, and compliance with, IG policies, standards, procedures and tools<br>• Facilitates adoption of IG practices and tools<br>• Synchronizes IG communication and training efforts across the agency |
| **Metrics and Measurement** | • Aggregates, organizes, and coordinates EOTSS's existing Key Performance Indicators (KPI's)<br>• Establishes metrics tied to IG strategic principles and critical success factors<br>• Creates a feedback channel with business units to monitor and understand IG risks, needs, goals, and opportunities<br>• Identifies opportunities to maximize information value and cost savings<br>• Takes place regularly to assess IG effectiveness and value consistently |

| IG Program Component | Description |
|---|---|
| **Compliance and Risk Management** | • Provides independent IG compliance controls<br>• Coordinated by the new Chief Compliance Officer and new IG Steering Group<br>• Addresses a critical but traditionally under-supported area<br>• Monitors IG-related legal and regulatory compliance<br>• Identifies emerging needs, gaps, or areas where incremental IG adjustments are needed |

## 5.3 IG Program Key Roles and Responsibilities

### Chief Compliance Officer

EOTSS IG Program will be led by a Chief Compliance Officer (CCO). The Chief Compliance Officer (CCO) will be independent from business units, solely assuming all responsibility related to IG compliance.

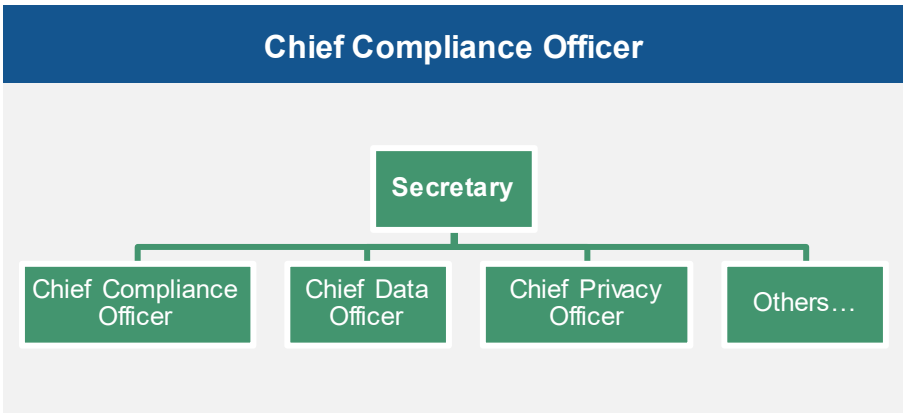



*Figure 3: IG Program Chief Compliance Officer Role*

The CCO will:

- Interface with the Secretary, IG Steering Group, business units, and other parties to incorporate IG direction and compliance across all IG-related efforts
- Appoint members to the IG Steering Group (IGSG) and chair said group
- Create compliance policies, communicate these across business units and staff via periodic training, and attest to compliance with these procedures
- Monitor compliance and risk, measuring and evaluating the level of compliance across the organization and investigating any violations of legal or regulatory requirements
- Secure executive sponsorship for IG from several constituents to ensure broad support for the recommended IG efforts and actions

## IG Steering Group

EOTSS IG Program will be collaboratively guided by an IG Steering Group (IGSG). The IGSG will be comprised of EOTSS Officers, serving as an advisory unit to the CCO and extending to operational/business units.

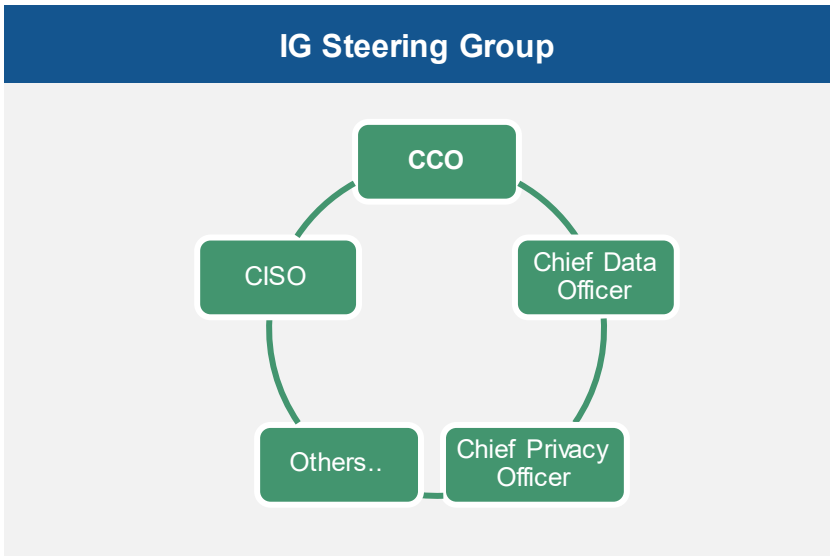



*Figure 4: IG Program IG Steering Group*

The IGSG will set the IG Program's strategic path and priorities, develop an ongoing implementation roadmap, recommend IG directives, establish policies and procedures, create training and communication materials, identify metrics for IG progress, and monitor IG compliance and risk management. Per the requirements outlined in the Budget, the above will be administered to the IG Functions of defensible disposition, offboarding, privacy and security, and lifecycle management.

Additionally, the IGSG will work towards identifying opportunities for cost savings and value optimization through the effective and efficient use of information assets, as well as resolve issues where conflicting IG-related policies, procedures, or practices are not in alignment with each other. The IGSG will also:

- Serve as an informational and advisory resource for the CCO, and extend his/her presence to the organization's operational units
- Perform regular assessment and prioritization of legal compliance risk areas, along with sharing of compliance program best practices. Formalize this process in annual reviews and oversight of people, process and technology
- Develop enterprise-wide tools and monitoring mechanisms to increase the efficiency and effectiveness of compliance activities
- Serve as a communication link between staff and the compliance function
- Determine the agenda and cadence (quarterly) for regular meetings across business units to ensure broad support for IG initiatives
- Collaborate with the existing RCB to leverage, for maximal compliance, the RCB's standards and guidelines for (electronic) records management

- Interface with other IG-related intra- and inter-agency or State councils and boards as necessary

## 5.4 IG Program Functional Areas (IG Functions)

Coupled with the creation of the CCO and IGSG, EOTSS's IG Program launch establishes launch activities associated with the following functional areas (IG Functions):

- **Defensible destruction**: regularly following procedurally defined activities to destroy or transfer information; resulting in a reduction of the cost and complexity of information retention and safeguarding against over-retention
- **Offboarding**: processes engaged when transitioning employees out of the enterprise that serve to effectively administer data/information associated with a given individual, ensure compliance with IG policies and procedures, and establish a culture of IG awareness and compliance
- **Privacy and security**: ensuring that the confidentiality, integrity, and availability of information assets are managed and protected in full compliance with all legal obligations and in accordance with EOTSS's Enterprise Information Security Standards
- **Lifecycle management**: identifying and implementing appropriate controls to create, use, maintain, access, and destroy/archive in alignment with EOTSS's legal obligations, Enterprise Information Security Standards, various systems, and strategic business goals

### Incrementally Addressing IG Function Complexities

Each IG Function presents unique needs around legal compliance, policies and standards, supporting procedures and/or tools, communication and training needs, goals for efficiency and economy, value/cost opportunities, and metrics for assessment. Additionally, each IG Function can overlap to present additional opportunities, or conversely, conflicts between competing compliance requirements, policies, or goals.

With the above in mind, it is imperative to plan and manage implementation and risk management activities around each function to ensure all goals are reasonably and realistically matched to the capabilities, capacity, and resources available to the enterprise.

*[Remainder of this page intentionally left blank]*

## IG Function Launch Activities

As detailed in the tables below, IG Program launch activities will primarily serve to establish alignment between the distinct IG Functions, the overall IG Program, and the recommendations previously established in collaboration with the Secretary of the Commonwealth under the "Electronic Records Management Guidelines." As necessary, the CCO and IGSG will collaboratively address gaps or updates in these materials.

To ensure alignment with IG industry resources and accepted best practices, launch activities are in general alignment with topics established in ARMA International's IG models. This strategic direction serves to:

- Root EOTSS's IG Framework in an agency-neutral structure and information
- Promote sustainability across EOTSS transformation and stakeholder transitions
- Realize guided, incremental advancement of IG maturity

|  **Defensible Destruction** | |
|---|---|
| **Key IG Program Launch Activities** | • Plan to establish a periodic review of information disposition efforts and procedures for compliance with the Statewide Records Retention Schedule to provide recommendations to the Records Conservation Board regarding amendments, when necessary<br>• Coordinate corporative and conflicting intersections around legal hold<br>• Work to incorporate IG activities into disposition to manage and control the growing volumes of both digital and physical information assets<br>• Plan to evaluate how defensible destruction can assisted by technology and integrated into all applicable data applications, repositories, and systems to manage the risk of over retention<br>• Work to establish regular reviews to assess records management goals being appropriately achieved and compliance with the Statewide Records Retention Schedule<br>• Determine the need for a documented, ongoing training program for all staff regarding the established document management policies and procedures including their responsibilities towards compliance<br>• Plan to establish and track KPIs to ensure compliance to IG-related policies and goals<br>• Work to establish review and continuous improvement processes to be formalized and monitored by the IG Steering Committee |

| Offboarding | |
|---|---|
| **Key IG Program Launch Activities** | • Institute processes to ensure personnel compliance with policies related to confidential data non-disclosure, equipment usage, etc.<br>• Outline security and mobile checklists for new staff (e.g., app privileges/access, etc.) and continually review the list of BYODs, their usage, and requisite hardware/software updates<br>• Determine existing centralized asset management systems' capacity to track all internal assets, their locations, and owners, and, keep an Electronically Stored Information (ESI) data map<br>• Develop processes to add non-standard software licenses/systems to the personnel file to ensure comprehensive management of assets during offboarding<br>• Work to identity appropriate controls over both formal and informal information and hardware (e.g., social media usage, BYOD, etc.)<br>• Augment the offboarding process to include transfer of IG responsibility to other staff, and ensure this obligation is seen as a vital component to that person's tenure<br>• Create a documented, ongoing "IG awareness" training program for all staff initially held during onboarding and administered on a regular basis<br>• Identify, monitor, and track all KPIs via a dashboard accessible to vital constituencies, with requisite staffing to handle all dashboard functionality and responsibilities<br>• Consider unified endpoint management systems – accentuating current controls and including new checks – to track arriving staff and weigh using a behavioral analysis solution to pinpoint high-risk activity patterns |

*[Remainder of this page intentionally left blank]*

| Privacy and Security | |
|---|---|
| **Key IG Program Launch Activities** | • Plan to incorporate a “privacy by design” approach to security where privacy and information protection are considered from the beginning of any project<br>• Establish an effort to evaluate the digital and physical assets recovery plan to help efforts to protect against information loss<br>• Work to establish an incident management plan which is regularly updated based on administrative and technological threat evolution<br>• Initiate a plan to establish a process to manage low risk information management issues to ensure timely management of all issues<br>• Evaluate the need to add a communication plan to the incident management program to ensure organizational transparency<br>• Work to establish a review to ensure all information assets meet metadata requirements including security, signature and chain of custody to prove authenticity<br>• Determine the need to supplement the existing ongoing training program for all employees, vendors and contractors with a training on:<br>  ○ Awareness to human security risks to mitigate human errors and reinforce behavioral expectations<br>  ○ Importance of privacy and individual responsibilities towards protection of information assets<br>  ○ Classification of information created and received<br>• Evaluate the list of measurable KPIs to ensure optimization of privacy and security efforts and spend across all IG functions<br>• Plan to conduct regular reviews to ensure all information assets adhere to the Commonwealth of Massachusetts Enterprise Information Security Policy |

*[Remainder of this page intentionally left blank]*

| Lifecycle Management | |
|---|---|
| **Key IG Program Launch Activities** | • Plan to consider IG efforts and compliance during procurement, information sharing with third parties, using data for analytics, and, implementing policies, procedures and technology (including existing software updates, emerging technology evaluation and implementation), etc.<br>• Initiate a plan to map all information assets, access restrictions and records retention schedule to support the IG Steering Group in creating a strategic plan and prioritizing IG areas of critical importance<br>• Establish an effort to evaluate taxonomies that will support IG-related policy and standards implementation<br>• Plan to validate if existing systems support established Electronic Records Management Guidelines policy requirements and procedures<br>• Work to establish roles and responsibilities regarding classification of sensitive information for all information assets<br>• Initiate a plan to integrate further metadata-related practices as a part of information management procedures<br>• Evaluate data storage locations to determine most efficient security level, and, IG-related policies and legal compliance requirements<br>• Assess if all employees are receiving ongoing, documented training on their responsibilities for compliance to information management policies and legal/regulatory requirements which include guidance on email management, social media, cloud and physical storage, etc.<br>• Evaluate potential review schedules to facilitate regular monitoring on compliance with policies and associated procedures<br>• Work to establish, track and monitor KPIs to ascertain a measurable return on investment on availability, retention and disposition of information assets<br>• Consider using content analytics to monitor, measure and evaluate the advantages of automation in managing the information lifecycle |

## 5.5 IG as a Continuous Process of Transformation

By establishing an IG Framework, EOTSS's aims to promote a sustainable and adaptable program to address the evolution of its information assets and leverage its existing investments in established IG-related areas. EOTSS views this as an evolving process that will incrementally and iteratively incorporate changes across our strategic goals, compliance needs, policies, standards, technologies, IG functions/components, and overall IG maturity.

**Balanced Activities**

Balancing multiple activities is key to launching and supporting a **sustainable, continuous IG program**

**Incremental Approach**

EOTSS's "launch and support" approach facilitates incremental **progress and transformation,** and enables additional phases for development and implementation

In parallel with the launch of the IG Program, the efforts of the IGSG and CCO, the EOTSS IG Framework will advance through additional phases to continue to:

- Harmonize IG with Commonwealth compliance requirements and existing EOTSS IG practices
- Coordinate IG across various EOTSS business units and functions
- Define new strategic IG principles to meet the Commonwealth's goals and needs
- Affirm existing IG roles and/or responsibilities, and establish new ones as necessary
- Define new, or identify needed, IG policies and standards
- Operationalize specific IG actions to realize EOTSS strategic principles, IG policies, and standards
- Articulate EOTSS's IG maturity and goals to enable ongoing IG development and measure continued progress

*[Remainder of this page intentionally left blank]*

# 6. Appendix

## 6.1 Definitions of Select IG Sub-Domains

- **Data Governance**: The Sedona Conference Commentary on Information Governance, Second Edition, cites the following definition for Data Governance, “The Data Governance Institute, self-described as a mission-based and vendor-neutral authority on essential practices for data strategy and governance, defines “data governance” as “a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.” ”

- **Data Quality**: NIST IR 7298 Revision 2, Glossary of Key Information Security Terms defines data security as, “Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.”

- **Identity and Access Management (IAM)**: Gartner defines IAM as a “Identity and access management (IAM) is the discipline that enables the right individuals to access the right resources at the right times for the right reasons. IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. IAM is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise. Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives.

- **Information Architecture**: Gartner defines information architecture as a “All the sources of information — including paper, graphics, video, speech and thought — that define the enterprise are represented by this layer of applications architecture. It also defines the sources and destinations of information, its flow through the enterprise, as well as the rules for persistence, security and ownership.”

- **Information Security (InfoSec)**: NIST IR 7298 Revision 2, Glossary of Key Information Security Terms defines InfoSec as “The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.”

- **IT Governance**: Information Governance for Business Documents and Records by Robert F. Smallwood defines IT Governance as, “Controls and process to improve the effectiveness of information technology; also, the primary way that stakeholders can ensure that investments in IT create business value and contribute toward meeting business objectives.”

- **Master Data Management (MDM)**: Gartner defines MDM as a "Technology-enabled discipline in which business and IT work together to ensure the uniformity, accuracy, stewardship, semantic consistency and accountability of the enterprise's official shared master data assets. Master data is the consistent and uniform set of identifiers and extended attributes that describes the core entities of the enterprise including customers, prospects, citizens, suppliers, sites, hierarchies and chart of accounts."

- **Metadata**: Association of Records Managers and Administrators International's (ARMA) Information Governance Body of Knowledge defines metadata as, "The structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage information resources."

- **Records Information Management (RIM)**: Association of Records Managers and Administrators International's (ARMA) Information Governance Body of Knowledge defines RIM as, "The field of management responsible for establishing and implementing policies, systems, and procedures to capture, create, access, distribute, use, store, secure, retrieve, and ensure disposition of an organization's records and information."

*[Remainder of this page intentionally left blank]*

# 7. Document Change Control

| Version No. | Revised By | Effective Date | Description of Changes |
|---|---|---|---|
| IG-2019-01 | EOTSS Secretary | 12/31/2019 | 12/31/19 EOTSS IG Framework |