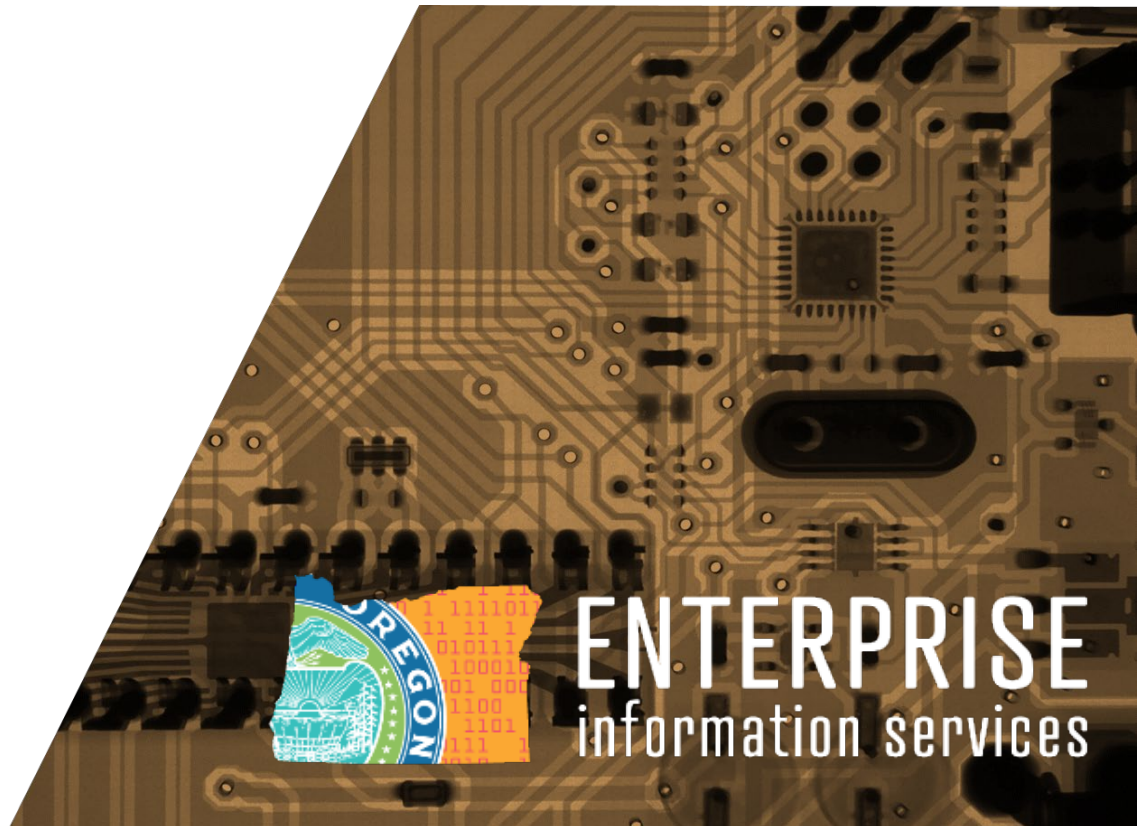


IT Governance Guide

2021

Agency Modernization – version 1.011



Contents

Introduction.....	2
Key Definitions.....	3
Overarching View of State IT Governance.....	4
Introduction to Strategic Governance	5
Initiation	7
Executive Driven IT Governance	7
The IT Governance Committee	8
Governance in Action	10
Decision Making	10
Monitoring Performance.....	11
Change & Communication	11
The Broader View of IT Governance.....	14
Assessing IT Governance	15
The Maturity Assessment.....	17
IT Governance Policy Template	19
IT Governance Charter Template	20
Appendix A. Reference	21



Introduction

As technology and business become more and more inseparable, state agencies of all sizes are acquiring better information technology solutions to solve business problems. Technology is inherently complex and the investment risks, as well as impact to business reputation, are often high.

Some of the factors contributing to increased complexity include:

- Expansion of business processes with greater degrees of automation
- Increase in the number of disparate systems supporting different parts of the business
- Adoption of modern or emerging technologies to improve user experience, provide flexibility, provide scalability, and increase the lifespan of systems
- A need for data sharing with external organizations and the public
- Managing relationships with a wider set of customers, policy makers, and an array of technology suppliers

Transformations carry with them substantial risks to an organization, and the use of well-established best practices is key to mitigating risk. “Information Technology (IT) governance” is an integral tool for agencies in their quest to modernize and improve the customer experience. Leadership, organizational structures, and processes are all elements of governance that sets out to ensure investment in information technology sustains and extends the organization’s strategy and objectives.

Effective IT Governance is a collaborative process that builds off long-range business plans, with the goal of reducing risks by ensuring resources expended in time, labor, and funding bring value. For the value to be realized agency leadership must effectively steer by determining the business goals and objectives, while the matching IT efforts need to be laser focused on execution to accomplish the agency goals and objectives. The basic framework of IT Governance is a common structure of planning and controls, and can be characterized by the following attributes:

- Formal executive endorsement through policy of the commitment and use of IT Governance
- Defined agency mission, goals, and vision statement
- Establishment of a decision-making body accountable for ensuring governance is viable and sustainable – often called a steering committee
- A method for making decisions and setting priorities; accounting for strategic alignment, value delivery, risk management, resource management, and performance management
- A “living” long-range plan used to communicate intent to employees, customers, and policy makers – often called an IT technology roadmap
- Continuous tracking, monitoring, and improvement of the IT Governance process to assure adaptability to changing business conditions

Governance solutions are not one-size-fits-all and need to be custom-tailored for each organization. The key is to embrace the lessons learned that are the basis for industry IT Governance standards.

Key Definitions

To ensure common understanding, listed below are terms to add context to establishing IT Governance.

- **Control Artifacts:** Documentation that records actions, tasks, and activities performed while carrying out agency's policies and procedures.
- **Executive Leadership Team:** The highest-level governing body charged with the responsibility to direct and/or oversee the agency's activities and hold senior management accountable.
- **Governance:** The combination of processes and structures implemented by executive leadership to inform, direct, manage, and monitor activities of the organization toward the achievement of its objectives.
- **Investments:** The planned or actual commitment of funds for IT-related expenditures. IT Investments include, but are not limited to, agency IT personnel, contracted labor, products, services, and contracts.
- **Information Technology (IT):** This includes, but is not limited to, all present and future forms of hardware, software, and services for data processing, office automation, and telecommunications.
- **IT Governance:** Consists of the leadership, organizational structures, and processes that ensure that information technology supports the organization's strategies and objectives.
- **IT Governance Charter:** Document defining the governance committee functions, roles and responsibilities, decision-making, prioritization, and oversight of IT strategy.
- **IT Governance Committee:** Control body, committee, or council to help mandate compliance with IT Governance objectives and establish investment priorities.
- **IT Governance Policy:** A policy, charter, and/or procedure approved by agency executive leadership that defines the roles and processes that an agencies IT Governance body/committee will follow.
- **IT Strategic Plan:** A business driven long-range plan, typically three to five (3-5) years in duration, outlining enabling technologies needed to achieve agency goals and objectives.
- **Risk Management:** Continuing process to identify, analyze, evaluate, and treat loss exposures and monitor risk control and financial resources to mitigate the adverse effects of loss related to technology.
- **Resources:** All equipment, networks, hardware, software, technical knowledge, expertise, labor, and other resources, including all computer systems, held, owned, or used by an agency.
- **Resource Management:** The process by which resources are manage effectively ensuring availability of appropriate resources to meet current as well as projected business demand.
- **Strategic Alignment:** Desired state in which organization can use information technology effectively to achieve business objectives.
- **Value Delivery:** Assessment and identification of business value with focus on maximizing quantifiable value of IT investments.

Overarching View of State IT Governance

In the digital transformation era, agencies have an opportunity to reinvent themselves and explore ways to place more emphasis on the mission of the organization. Embracing a new strategic approach to collaboratively work with other agencies and the enterprise is one way to decouple the amount of energy and investment placed on technology. Leveraging enterprise pricing for commonly consumed items and economies of scale can work to the advantage of an agency by narrowing focus to the few unique services the business requires. To make this work a three-tiered IT Governance structure separates while still binding the agency and enterprise into a cohesive team that coordinates the allocation of resources, in lieu of competing for them. Alignment is needed between the various levels of governance to help sustain and adapt to business needs while simultaneously striving for clear outcomes. The graphic below is intended to convey the pathways and connected collaboration to the benefit of all stakeholders.



Figure 1: Holistic view of Oregon State IT Governance

- **Enterprise Governance:** The Governor’s IT Action Plan sets the vision for the Executive Leadership team, the state Chief Operating Officer, and the State Chief Information Officer on long-term policy planning.
- **Enterprise IT Governance:** Enterprise IT Governance Committee (EITGC) and Enterprise Information Services (EIS) teams come together seeking to find ways of reducing risks, as well as cost and economies of scale opportunities.
- **Agency IT Governance:** Strategic planning and prioritization of technology investments best supporting the agency mission.
 - **Executive Team:** Commitment by agency leadership, accountability for the success of change, embodiment or role model for change, and willingness to challenge long-standing assumptions and institutions.
 - **IT Governance Committee:** Agency wide strategic planning governance framework presented by this guide that is adopted by charter and operationalized through agency policy.
 - **IT Investment Committee (optional – often part of an IT Governance Committee):** Guides the work and more operational in focus as it prioritizes the resulting body of work IT is assigned through strategic planning phase.
 - **Program and Project Committee:** Governs projects or programs that are under EIS oversight. EIS Senior IT Portfolio Manager are non-voting member of chartered project or programs.

Introduction to Strategic Governance

Taking a strategic approach to implementing IT Governance helps agencies address the speed of technological advancements, IT services proliferation, and the greater dependency on IT to meet organizational objectives. Effective IT Governance contributes to efficiency and effectiveness and allows the agency's investment in IT to realize both financial and nonfinancial benefits. Often when controls are poorly designed or deficient, the root cause is weak or ineffective IT Governance.

To that end, the use of "tried and true" methods yields the best result while simultaneously providing for common understanding. EIS relies on a standard framework called, "Control Objectives for Information and Related Technologies", or better known simply as COBIT®, to define the basics of good governance.

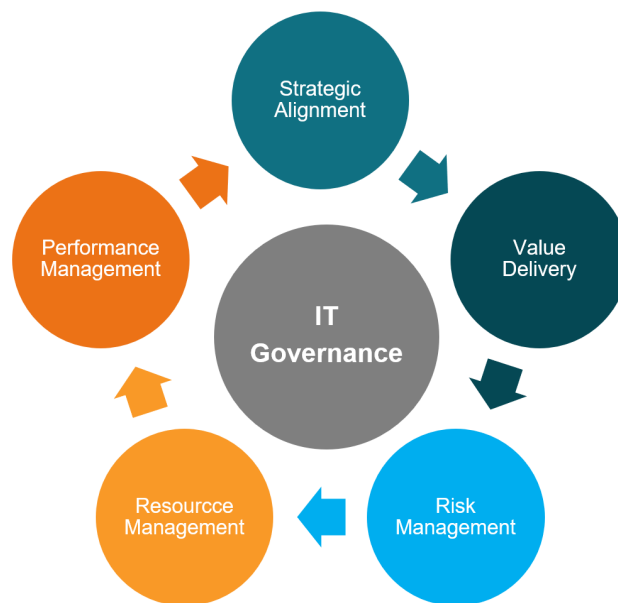
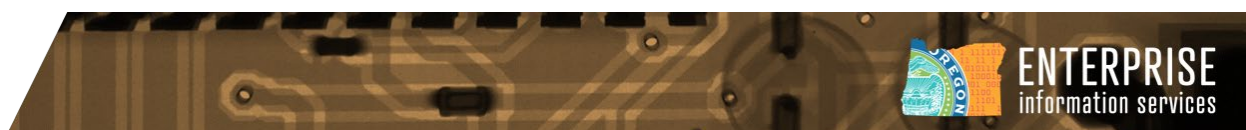


Figure 2: ISACA COBIT® IT Governance Framework

- **Strategic Alignment** - The strength of the linkages between an agency's overall vision, mission and values has a direct relationship to the success of achieving overall goals. Creating IT strategic alignment ensures projects and processes are working in sync and are contributing to long-term success of the business. The complexity of alignment increases when goals and accountability become delegated below the executive leadership level as measurements of business/IT alignment become less certain. Therefore, it is important for strategy to be business-led in order to accurately measure outcomes.
- **Value Delivery** - This consists of creating value for the agency through IT, maintaining and increasing value derived from existing investments, and eliminating initiatives and assets that are not creating sufficient value. The basic principle of IT value are delivery of fit-for-purpose services and solutions, on time and within budget, that generate the intended financial and nonfinancial benefits. The value that IT delivers should be aligned directly with the values on which the business is focused. IT value should also be measured in a way that shows the impact and contributions of IT-enabled investments in the value creation process of the enterprise.

- **Risk Management** - Entails addressing the business risk associated with the use, ownership, operation, involvement, influence and adoption of information technology within an organization. IT business risk consists of “IT-related” events that could potentially impact the business. While value delivery focuses on the creation of value, risk management focuses on the preservation of value. The management of IT-related risk should be integrated within the agency risk management program to ensure there is a focus on IT initiatives and operations. Risk should also be measured in a way that shows the positive impact and contributions of optimizing IT-related business processes that preserve value.
- **Resource Management** - Ensures appropriate capabilities are in place to execute the strategic plan and sufficient, appropriate, and effective resources are provided. Resource management ensures that an integrated, economical IT infrastructure is provided, new technology is introduced as required by the business, and obsolete systems are updated or replaced. It is important to recognize people, in addition to hardware and software, by focusing on providing training, promoting retention, and ensuring competence of IT personnel. Another important resource is data and information and exploiting data and information to gain optimal value is another key element of resource management.
- **Performance Management** - Performance management represents a general term for measuring all activities and resources consumed that lead towards achieving strategic outcomes. It expresses how well the governance and management system, as well as the IT operations of an agency work, and how they can be improved. It includes concepts and methods such as capability levels and maturity levels that become the basis for EIS assigning an Agency Maturity Score associated with Information Technology Investment Oversight.

Agencies are unique, and many already have elements of IT Governance in place. The basics of the governance described in the following sections seeks to unify and clarify key processes, principles, legislative deliverables, and expected enterprise outcomes within agency modernization efforts.



Initiation

The primary questions that need to be answered as IT Governance is established are:

- What decisions must be made?
- Who will make these decisions?
- How will decisions be made? and
- What is the process for monitoring results?

The intent of the following sections is to cover key process areas directly impacting Agency IT Investments as outlined within EIS Maturity Assessment Process, and agencies should consult the EIS Modernization Playbook for a full primer on institutionalizing sound IT Governance practices.

Executive Driven IT Governance

Direction and success starts with executive leaders establishing the mission, vision, and values of an organization. Policies also serve a vital role in strengthening, supporting, and protecting an organization and its people and they help to form boundaries and serve as guides.

Agencies should establish a policy where Information Technology (IT) decisions are governed through a formal IT Governance process. This provides structure to ensure IT investment decisions are driven by strategic planning, support business objectives, and align with EIS technology strategies.

The agency IT Governance policy should clearly specify the criteria and thresholds for IT investments, and the criteria should align with Enterprise Governance thresholds to ensure consistency.

Key elements to incorporate into IT Governance policy include:

- Agency Executive Director denoting accountable for creating and adopting an agency IT Governance Policy.
- Purpose and policy statement outlining the intent as it relates to agency:
 - IT strategy
 - IT investments; and,
 - Establishment of a business-led decision-making body
- Periodic basis for which the Agency is to assess conformance to the policy, and associated performance or success factors.
- Specific circumstances for exclusions or special exceptions to the policy, including who has the authority to grant the exclusions and special exceptions.
- Annual review of the Agency IT Investment Governance Policy and Procedure.

For an effective IT Governance Policy to work a procedure should be established as well. The Procedure documents the processes by which the policy will be implemented, and includes the following types of information:

1. The IT Investment request initiation process.
2. The IT Investment request review and approval process.
3. The IT Investment prioritization process.
4. Roles and accountability within each process.

5. Relation to Enterprise IT Strategic direction.
6. Process for recording and retaining information related to each process.
7. Exception process information.

For more information about establishing an agency IT Governance Policy and procedure, see the Policy template included with this guide. Additionally, Assistant State Chief Information Officers (ASCIO) are available for consultation in the development and adoption of the IT Governance policy. Per the Agency Maturity Assessment Procedure, EIS will review adopted policies and revisions for completeness, as well as the policy conformance and performance in supporting agency business objectives, oversight maturity assessments, and Enterprise Information Technology Strategies.

The IT Governance Committee

A key component of IT Governance is establishing a decision-making body, more commonly known as the IT Governance Committee (ITGC), for an agency. The ITGC is a body comprised of business leaders and subject matter experts within an agency that is supported by policy, chartered, vested with authority, capable of making decisions, setting standards, and mitigating IT risk. Typically, this is a distinct body set up for the purpose of IT Governance, yet in smaller organizations this function may reside within an existing body, such as an agency's Executive Leadership Team.

Purpose/Value:

The ITGC gives the agency the capability to:

Align and be responsive: Works hand in hand with IT portfolio management to align IT investments with agency objectives, enabling improved responsiveness to challenge and management of current and future IT investments. It provides transparency to agency IT investments and ensures resources are spent in accordance with the agency's mission.

Objectively make decisions: Allows leadership to actively commit to improving the management and control of IT activities in the agency.

Balance resources: Proper management of critical resources enables control in planning and organizing IT initiatives. This gives management the ability to ensure adequate IT support is available for current and future IT investments.

Manage organizational risk: Proactive risk management ensures leadership is aware of the risk associated with the IT initiatives and provides the basis to implement risk mitigation strategies.

1. Creating a Charter:

- Start by describing the scope of ITGC authority
 - Include the appropriate level of authority and access within the agency to make decisions, as well as policies related to IT strategy, prioritization, and oversight
- Describe roles and responsibilities of committee members within the agency
 - It is recommended the senior most executive retains a leadership position as the Chair, include high to mid-level business executives, the CIO or Technical Lead, as well as the CFO or Finance Lead



- Additionally, include as non-voting members the Assistant State CIO and Senior Information Portfolio Manager (SIPM) from within the EIS Policy Area
- Ensure a designation is made for providing logistics and capturing the work of the committee
- Make accommodations for business and technical subject matter experts on an as needed basis
- Outline basic committee functions including, but not limited to:
 - Frequency of meetings
 - Standard meeting procedures
 - Supporting Information: meeting minutes, decision log, performance reports, IT strategic plan

2. Form a sustaining Committee

Achieving agency goals and objectives have a longer time horizon, and ensuring committees regularly meet is essential in building up trust in the process and realizing the resulting value. Setting up the ITGC takes effort. Below are a few foundational items to be developed:

- IT Strategic Plan that serves as a guide to IT-related decision making and provides a sense of direction and outlines measurable goals
- A prioritized IT investment portfolio where all projects are viewed in relation to one another, not on a standalone basis.
 - High-risk projects are balanced with low risk, and short term with long term
 - Follows the same principles as those employed in managing a financial portfolio
 - Includes IT investments meeting thresholds to be governed by EIS/P3 and QA policies
- An IT dashboard and reports for tracking performance.
 - Helps stay on top of IT projects and track vital milestones, risks, and issues
 - Efficiently track relevant IT cost details

It should be noted that the formation of an ITGC within an agency is directly tied to state-wide modernization goals presented in the EIS's Strategic Framework, which purpose is to assist with the legislative process. Specifically, Objective #3, Goal #1, which states: "80% of agencies will have a formal IT Governance procedure and a functioning IT Governance Committee implemented by December 31st, 2022".



Governance in Action

Effective IT Governance requires a mature, stable overall governance structure and strong, well-functioning committee. The focus should be on achieving results from strategic choices and helping the IT investment leaders and stakeholders navigate through the most challenging financial and implementation issues. Enhancing value creation by getting the most out of the IT portfolio requires making difficult decisions about how to allocate finite resources among all the potential opportunities and then sequencing the ones that are approved. The agency needs to be accountable for the delivery of value from IT-enabled operational capabilities.

Decision Making

With respect to technology there are five major decision domains related to the high-level decisions connected to the strategic role of IT in the business.

- **IT Principles:** Strategic use of IT requires the members of the IT Governance Committee to specify the agency long-term operating model and any other directives clarifying the role of IT within the agency. Governance allocates decision rights determined based on established IT principles -- usually to one or more members of the senior management team. The principles give guidance, such as emphasis on simplification, usability, integrated workflows, single sources of data, Cloud-first polices, etc.
- **Elements of Architecture:** Includes an integrated set of technical choices to guide the organization in satisfying business needs. Refers to the design of the agency digital platform and specify the people responsible for establishing business process, data, and technology standards, and for dealing with requests for exceptions to those standards.
- **IT Infrastructure:** Trade-offs between directly building, operating, and maintaining IT infrastructure versus leveraging common cost-effective Shared Services available to all parts of the enterprise. The IT Charter is to designate responsibility for defining and assessing pricing of IT shared services.
- **Business needs and Project Deliverables:** New systems and processes emerge from an extended agency effort that starts with a business case for a new system and ends, ideally, with a review of the outcomes of that system implementation. The IT Charter is to assign ownership for defining the business case, ensuring successful implementation, and delivering the benefits.
- **IT Investment and Prioritization:** Lastly, prioritization and investment decisions determining how much and where to invest in IT. Although critical, IT investment and prioritization are just one of five IT decisions that needs to be governed.

Each of these decision areas can be addressed at many levels: enterprise level, business unit or functional level, or some combination of the three, and senior management can hold business unit or IT leadership accountable for the related outcomes. Thus, the charter determines who should make and be held accountable for each decision area.

- **Decision Making Processes:** Within the procedures of the IT Governance Committee, the decision-making processes are established to secure effective involvement of the members chartered specifically for this purpose. The following are common decision-making processes to be detailed within the governance charter and adopted.
 - Establishing an IT investment proposal process; this process delineates steps for defining, presenting, reviewing, and prioritizing IT investments. (For example, starting with an IT investment and budgetary business case documentation).

- Based on a consistent formalized “prioritization” framework, determine which projects will be funded and identify/designate method of funding.
 - Allow for an Architecture-exception processes; evaluate formal assessment of the cost, impacts, and value of IT project proposals that veer from enterprise standards.
 - Service level agreements, associated operational costs, and contract performance is regularly evaluated and compared with the business need.
 - Formally track the business value from IT investment through cost benefit (CBA), return on investment (ROI), return on equity (ROE) or return on asset (ROA) whichever is selected to be appropriate for the business.
- **Decision Log:** Tracking choices demonstrate the level of maturity of the IT Governance process. As support for determination of maturity level, a decision log should include the following minimum set of information:
 - Description of what the decision relates to: prioritization, selection, issue, risk, performance, change, strategy, etc.
 - Details about what was decided on: CBA, ROI, Business Case and other forms of decision justification documentation.
 - Who made the decision; and,
 - When the decision was made

Monitoring Performance

For agencies it is crucial to receive value for every dollar invested in technology. This requires a focus on performance and the removal of non-value-adding activities and processes. IT Governance performance monitoring can be defined as the area of setting goals, responsibility accounting and monitoring / analyzing / governing and improving the performance of IT.

- Viability and performance of both agency IT Governance and the ITGC is to be reviewed regularly for key governance elements, including but not limited to:
 - Setting and maintaining an agency IT strategic vision.
 - Quality of decision-making.
 - Responsiveness to agency IT needs.
 - Effectiveness of and adherence to standardized governance procedures.
 - Modernization following established technology roadmaps.
 - Performance and continued operation of the ITGC; and,
 - Participation in the EIS/P3 annual Agency Governance Maturity Assessment

Change & Communication

Effective communication ensures that all members of an organization are aware of the decisions being made, progress towards goals, its importance and how they might be impacted. After all, to achieve success, a strategic plan relies on the activities of many people in an agency -- not just the committee or planning team.

- Change:** Change communication is the informational component of a change management strategy that helps stakeholders understand what is changing and why, and how it will specifically affect them. It delivers timely messages and materials aligned with key milestones, ensures stakeholders receive consistent information about what is important to them, and provides a mechanism to share feedback and ask questions.

Creating a change management plan for IT Governance starts with an understanding of the organization, stakeholders and change impacts. The goal is to support the business objective by helping stakeholders understand the change, how they will need to adapt their day-to-day responsibilities and what is expected of them from the IT policy.



Figure 3: Change Management Framework

By ensuring a consistent flow of information, engaging stakeholders and continually managing feedback, change communication helps people feel more comfortable as they move to the future state of modernization and adopt new ways of working.

- Communications:** A significant barrier to effective IT Governance is lack of understanding about how decisions are made, what processes are being implemented and what the desired outcomes are. Agency management can communicate governance processes in a variety of ways, and best practice is to ensure IT policy is drafted and adopted as a first step. Then, establishing a consistent cadence for publishing governance information in a cascading manner will result in effective communication that reaches throughout the organization.

Adopting use of a communication plan helps describe how information keeps stakeholders informed. The following diagram illustrates the concept of a common communication framework for IT Governance, which will vary based on size and complexity of an agency.

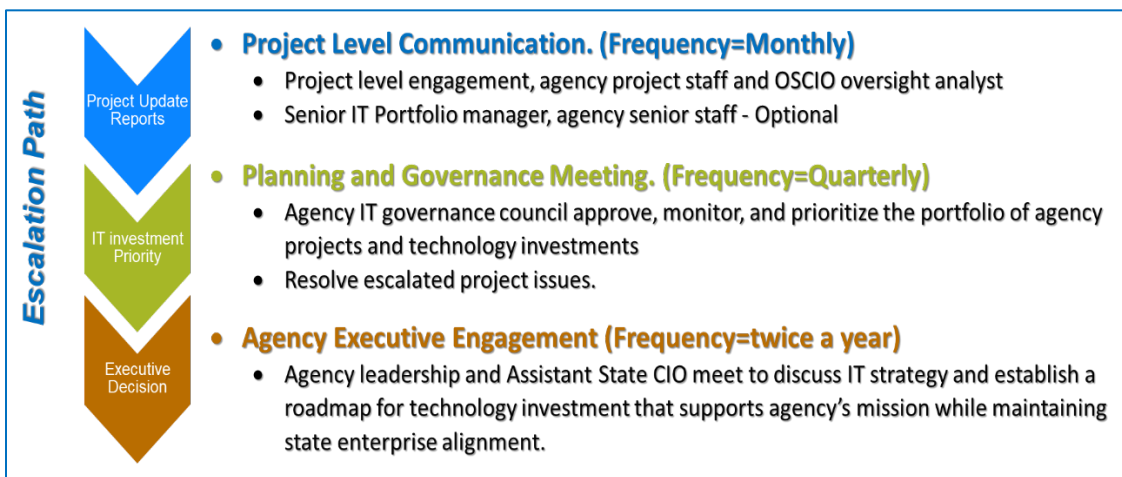


Figure 4: Example Communication Framework

- **Communication Framework:** Activity at various levels of IT Governance is the basis for the communication framework listed on the diagram above, and can be described as follows:
 - **Project level communication:** This activity is typically performed on a frequent basis, typically weekly or monthly, and can be adjusted depending on level of risk or volatility of a project. The EIS Senior Oversight Analyst and agency project management team will make the determination of the reporting period.
 - **Planning and governance:** This activity is typically completed on a monthly or quarterly basis. The IT committee reviews, prioritizes, approves, and monitors the agency IT portfolio and new technology investment opportunities, and resolves escalated project issues.
 - **Agency executive engagement meeting:** This activity is performed at least twice a year. Agency leadership and Assistant State CIO meet to discuss IT strategy and review the established roadmap for technology investment opportunities that support/enhance the agency mission, while ensuring there is enterprise strategic alignment.

Communications of governance processes and outcomes are effective when shared widely with the business and IT community, as well as with business leadership affected by the management of information technology. Regular communications regarding key governance activity, policies and decisions should be published on the agency public website and reported to key leadership groups that regularly meet for information sharing (e.g., cabinet meetings, deputies' meetings, Legislative Fiscal Office meetings, etc.).



The Broader View of IT Governance

Creating a viable IT Governance takes more than creating committees and strategy documentation against a rigid standard. It takes incremental steps evaluating people, processes and technology all working together. Real governance solutions are custom-tailored for the need, and a key step is understanding where an agency governance processes are on the maturity curve, and what strengths it has that can be leveraged. Understanding this can help with designing/modifying a governance approach that is tailored to the agency and fits within its cultural norms.

It should be of no surprise to find that IT Governance spans IT functions as a whole and can be adapted to meet the unique organizational needs. As demonstrated below, a holistic view of control points would of course vary in breadth and scope based on the size and complexity of an agency yet is consistent with the best practices of the COBIT® framework.

		PEOPLE	PROCESSES			TECHNOLOGY
		Human Capital	Organizational Bodies	Organizational Roles	Organizational Tools	Technologies & Tools
IT Governance	Strategic Level	<ul style="list-style-type: none"> Agency Culture Values Beliefs Behaviors 	<ul style="list-style-type: none"> Executive Leadership Team IT Steering Committee 		<ul style="list-style-type: none"> IT Strategy Policies on IT Data Governance Information Security Controls 	<ul style="list-style-type: none"> Organizational plans IT Balanced Scorecard Service Level Oversight
IT Management	Tactical Level	<ul style="list-style-type: none"> Skill set Sourcing Strategies 	<ul style="list-style-type: none"> Change Control Board 	<ul style="list-style-type: none"> Chief Information Officer Program/Project Managers Unit Managers 	<ul style="list-style-type: none"> IT Standards and Policies Security baselines Project Management Methods Services Level Management 	<ul style="list-style-type: none"> Multiple Unit IT Balanced Scorecard Project Metrics Application Systems Metrics Service Level Agreements
	Day-to-Day Operations	<ul style="list-style-type: none"> Training Awareness Compliance Continuous Improvement 	<ul style="list-style-type: none"> Other collective management bodies 			

Figure 5: IT Governance Control Points



Assessing IT Governance

IT governance is directly related to organizational oversight of IT assets and risks, making it a shared responsibility of the agency and the Enterprise. As such outcomes of effective IT Governance need to be regularly assessed from both the agency and the Enterprise perspectives.

Agency Perspective

As denote by the ITGC Charter, following policy and providing oversight of investments, managing risks, and monitoring performance are integral to the committees' accountabilities. This allows for the agency to monitor success while adjusting as the business environment changes. Agencies should establish criteria to ensure intended outcomes are clear and provide value or provide early warning signs when IT Governance needs improvement. Use of basic tools such as SWOT analysis, benchmarking, focus groups, and brainstorming are all viable methods for assessing IT Governance performance.

Enterprise Perspective

“The State Chief Information Officer shall oversee and coordinate the planning, budgeting, architecture and standardization, consolidation, acquisition and oversight of all information and telecommunications technology by state government and agencies of state government so that statewide and individual state agencies’ plans and activities are addressed in the most integrated, economic and efficient manner, in a manner that minimizes duplication, fragmentation, redundancy and cost in state government operations and in a manner that most effectively meets state government and state agency program needs.”

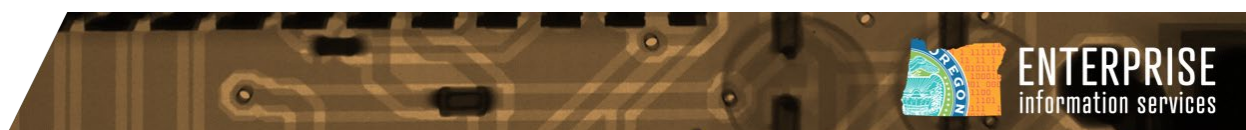
ORS 276A.206

At the enterprise level state statute directs the State Chief Information Officer (CIO) to both oversee and coordinate technology investments by state agencies to increase efficiency and reduce redundancy and cost.

This governance includes the processes of monitoring, controlling, and provisioning resources for IT investments. Accordingly, part of the State CIO’s responsibility includes developing awareness of state agency governance processes and effectiveness. This awareness provides both an opportunity to improve governance statewide and to inform the level of individual IT investment oversight required of agencies.

Towards this end, EIS maintains a Maturity Assessment for all agencies subject to oversight as prescribed in Information Technology Investment Oversight Policy, 107-004-130.

This assessment includes numeric representations of maturity relating to agency IT Governance (aligned with COBIT® capability levels), Project and Portfolio Management Organizational Structure, and Oversight Experience. Reference the EIS Maturity Assessment Process. The Maturity Assessment informs the oversight level for all IT investments requiring oversight.



IT Governance Maturity

EIS reviews both strategic and operational documented agency governance artifacts (e.g., policies, procedures, charters, decision logs, roadmaps) with particular focus on effectiveness, adherence, and alignment.

The basis for assessing an agency maturity relies on COBIT® 2019 Maturity Levels for Focus Areas and Capability Levels for Processes:

Maturity Assessment Score	Description
5	<p>Optimizing—The enterprise is focused on continuous improvement. The process achieves its purpose, is well defined, its performance is measured to improve performance and continuous improvement is pursued.</p>
4	<p>Quantitative—The enterprise is data driven, with quantitative performance improvement. The process achieves its purpose, is well defined, and its performance is (quantitatively) measured.</p>
3	<p>Defined—Enterprise-wide standards provide guidance across the enterprise. The process achieves its purpose in a much more organized way using organizational assets. Processes typically are well defined.</p>
2	<p>Managed—Planning and performance measurement take place, although not yet in a standardized way. The process achieves its purpose through the application of a basic, yet complete, set of activities that can be characterized as performed.</p>
1	<p>Initial—Work is completed, but the full goal and intent of the focus area are not yet achieved. The process achieves its purpose through the application of an incomplete set of activities that can be characterized as initial or intuitive—not very organized.</p>

*COBIT® 2019 Framework: Introduction and Methodology, Chapter 6 Performance Management in COBIT, Figures 6.2 and 6.3
Note: Level 0 – Incomplete has been removed for simplicity*



The Maturity Assessment

Monitoring and assessment of IT Governance viability can be performed by verifying key processes and measures in place to ensure successful outcomes. To do so EIS uses the standard set of question below derived from the COBIT® framework. This allows agencies to self-assess and identify opportunities for improvement in their IT Governance and is also the basis for assigning an IT Governance Maturity Score by EIS in a transparent manner.

1. ORGANIZATIONAL AND GOVERNANCE STRUCTURES

The following questions will help gain an understanding of the degree or presence of IT Governance:

- Is there a full-time CIO/Technical Lead in place, and is this function a member of the senior management team?
- Is the structure of the agency and its operational components clearly organized such that the IT function can efficiently and effectively help enable the achievement of the organization's objectives?
- Are decision-making bodies in place to enable alignment of organizational needs with IT services, and do they have adequate empowerment and accountability?
- Are organizational needs and IT service requirements defined in strategic and tactical plans, and monitored?
- Does the CIO/Technical Lead and senior management meet and discuss progress on plans on a regular basis?
- Are roles and responsibilities clearly defined and communicated, and are organization leaders empowered and held accountable for results?

2. EXECUTIVE AND LEADERSHIP SUPPORT

The following questions will help assess the degree to which the IT function is integrated into the organization:

- Does senior management have clearly defined and communicated roles and responsibilities for the IT function with respect to the organizational achievement of strategic and tactical goals?
- Are the roles and responsibilities of the CIO/Technology Lead clearly defined and communicated?
- Does the organization recognize in its strategy that the IT function is a significant contributor in enabling the achievement of goals, as well as supporting the organization on a day-to-day basis?
- Does the CIO/Technology Lead meet with the board and the senior management team on a regular basis to discuss IT service delivery related to strategic and tactical plans?
- Does IT have adequate funding to meet the organization's needs?

3. STRATEGIC AND OPERATIONAL PLANNING

Assessment of how well strategic performance management has been implemented by senior management by asking the following questions:

- Does the agency Director and senior management view IT as a strategic organizational partner?
- Does the strategic plan of the organization include how IT is required to support and enable value creation?
- Is the strategic plan supported by individual tactical operating plans that consider IT requirements and deliverables?
- Are key performance indicators (KPIs) used by senior management to measure and monitor the effectiveness of the IT function?
- Are strategic IT investment decisions based on accurate cost benefit analyses and evaluated after implementation to determine whether the projected ROI has been realized?
- Are lessons learned factored into future IT investment decisions?
- Is the IT organization structured effectively relative to the size and composition of the organization?
- Are the CIO and IT leadership qualified and experienced?

4. SERVICE DELIVERY MEASUREMENT

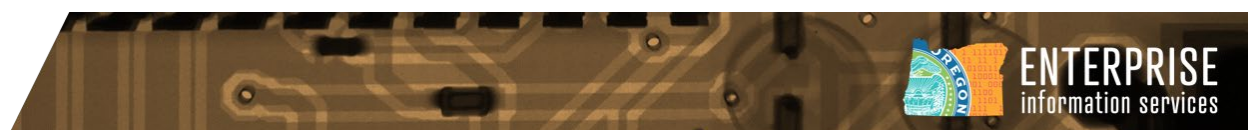
Assessment of how well financial management of IT is functioning by asking the following questions:

- Does the senior management have a clear understanding of IT costs and how they contribute to the achievement of the organization's strategic objectives?
- Do leaders of the organization measure IT value and deliverables?
- Are IT costs compare to other comparable organizations?
- Is CIO/Technical Lead performance measured by financial and nonfinancial data?
- Are there procurement sourcing arrangements in place, and are they measured and monitored?

5. IT ORGANIZATION AND RISK MANAGEMENT

Assessment of the IT Governance environment by asking the following questions:

- Are organizational processes automated and workflows integrated?
- Are the mission critical applications formally known and have an associated lifecycle plan?
- Is data standardized and easily shared across applications (and the IT infrastructure)?
- Are there standard IT hardware, software, and service procurement policies, procedures, and controls in place?
- Are IT management processes mature, and are recognized frameworks used (e.g., COBIT, ITIL, ISO)?
- Are risks managed in relation to meeting organizational needs, security, and compliance requirements?
- Is the strategic importance of IT risk management defined?



IT Governance Policy Template

Below is a standard outline for an IT Governance Policy that can be incorporated into an Agency standard template for consistency or optionally use the example down below.

Policy Outline

1. Purpose
2. Applicability
3. Definitions
4. Authority (optional)
5. Policy
6. Roles and Responsibilities
7. Standards
8. Exceptions and Exclusions
9. Supporting References
10. Review Interval

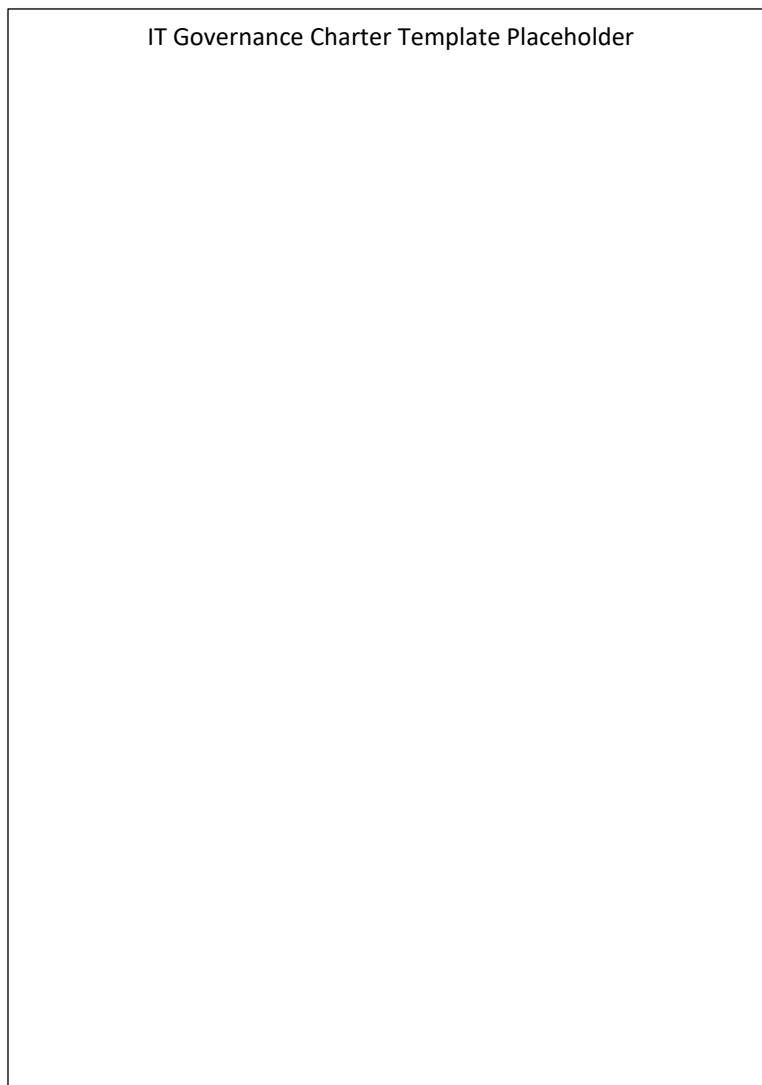
IT Governance Policy Template Placeholder

IT Governance Charter Template

Below is a standard outline for an IT Governance Charter that can be incorporated into an Agency standard template for consistency or optionally use the example down below.

Charter Outline

1. Purpose
2. Expected Results
3. Approach
4. Operating Principles
5. Decision Making
6. Roles & Responsibilities
7. Membership
8. Approvals



Appendix A. Reference

COBIT 2019

[COBIT | Control Objectives for Information Technologies | ISACA](#)

Global Technology Audit Guide

[GTAG | Auditing IT Governance | IIA](#)

Agency Maturity Assessment Procedure

[Agency Maturity Assessment Procedure](#)