Information Technology Advisory Council (ITAC)
December 11, 2024 – 1:00 pm

Virtual meeting: WebEx link on Virginia Regulatory Town Hall

Agenda

Call to Order and Welcome	
Rollcall	**Staff**
Review of Agenda	**Staff**
Approval of Minutes	**Staff**
Cyber Governance	**Amy Braden, Director of Security Governance VITA**
IT Planning in the Executive Branch & Six-Year IT Modernization Plan	**Robert Osmond, CIO of the Commonwealth**
Other Business	
Adjourn	

Information Technology Advisory Council

August 8, 2024 – 1pm

VITA, Mary Jackson Boardroom

MEETING MINUTES

Call to Order and Welcome:

The meeting was called to order at 1:20pm by Ms. Kozanas. Ms. Kozanas welcomed back the members and welcomed guest speaker Dan Wolf.

Mr. Heslinga noted as follows:

> This meeting of the ITAC is occurring during a declared state of emergency, pursuant to Governor Youngkin's Executive Order 34 (effective August 6, 2024). ITAC includes members at considerable distance from the central, physical meeting location. It is impracticable or unsafe due to the nature of the emergency to require physical attendance to assemble a quorum in the physical location. And the purpose of this meeting is to provide for the discharge of ITAC's lawful purposes, duties, and responsibilities.
>
> All meeting materials are available through the Agenda link on the page for this meeting on the Virginia Regulatory Town Hall. Necessary information to attend the meeting virtually is also available there. Both were fully available to the public on Monday, August 5. The public has had an opportunity to join this meeting virtually (as with all ITAC public meetings), and there was an opportunity to provide public comment during the customary times (virtually by email as well as in-person today).
>
> Accordingly, the requirements of Virginia Code § 2.2-3708.2 are met, and this meeting is being held without the requirement for a physically assembled quorum.

Presiding:

Dena Kozanas, Vice Chair

Members present in-person:

Secretary of Administration Lyn McDermid

Chief Information Officer of the Commonwealth Bob Osmond

Commissioner Melis (designee of Sec. Slater)

Phea Ram

Delegate Michael Feggans

Adam Lee

Members participating remotely:

Dena Kozanas

Delegate Marty Martinez

Senator Saddam A. Salim

Senator Bill DeSteph

Senator Jennifer Boysko

Delegate Kannan Srinivasan
Delegate Joshua Thomas
Sam Nixon
James Kraemer
Anthony Gitalado

Members Not Present:

Robert Turner
Dr. Timothy Tillman
John Craft
Cherif Kane

VITA Personnel Present

Naveen Abraham, Chief of Core Infrastructure Services, Virginia IT Agency
Mike Watson, Deputy CIO & Chief Information Security Officer, Virginia IT Agency
Melinda Stewart, Chief of Enterprise Solutions, Virginia IT Agency
Richard Matthews, Chief of Customer Experience, Virginia IT Agency
Chris Hinkle, Director, Oversight and Governance, Virginia IT Agency
Stephen Smith, Acting Director, Enterprise and Security Architecture, Virginia IT Agency
Amy Braden, Director, Security Governance, Virginia IT Agency
Jessica Sudduth, Director, Customer Relationships, Virginia IT Agency
Joshua Heslinga, Director, Legal and Legislative Services, Virginia IT Agency
Sam Taylor, PR & Marketing Specialist ,Virginia IT Agency
Patrick Disney, Coordinator, Virginia IT Agency
Amy Judd, Records Management and Compliance Specialist, Virginia IT Agency

Review of Agenda

Mr. Disney provided an overview of the agenda.

Approval of Minutes

The December and April meeting minutes were displayed on the screen. Upon a motion by Mr. Lee, seconded by Mr. Ram, the Council unanimously voted to adopt the meeting minutes.

Approval of Electronic Participation Policy

The policy was displayed on the screen. Upon a motion by Commissioner Melis, seconded by Mr. Lee, the Council unanimously voted to adopt the updated electronic participation policy.

IT Modernization in Other States

Dan Wolf, Director of State Programs at the Alliance for Digital Innovations, presented on IT modernization in the federal government and on the state level. (A copy of his presentation is available in the meeting materials.) He discussed the benefits of modernization, public sector IT funding mechanisms, federal grant funding, and the US Tech Mod Fund. He covered multiple states, describing what they are currently doing to modernize IT and how the states provide for funding modernization. Key takeaways were that there is no "one size fits all" approach, stakeholder involvement and commitment are essential (including both legislative and executive), and strategic planning is a must. Questions included whether there is any current state collaboration in effort to save money, and whether there is always a blank slate or is there an ongoing product backlog list of issues.

Project Management Governance

Chris Hinkle presented on governance and oversight of projects for executive branch agencies. (A copy of his presentation is in the meeting materials.) The presentation addressed governance models, risk management, and strategic planning steps from start to finish. Defining processes, good relationships with agencies, and development programs were all mentioned as accomplishments. High risk projects, understaffing, and improving risk management were mentioned as areas for improvement. Questions included how state project managers are certified, alignment with private project management programs, and mechanisms for projects not to fail.

Enterprise Architecture Governance

Stephen Smith presented on the EA standards, roadmaps, and governance. (A copy of his presentation is in the meeting materials.) He described what EA does and the core standards. Areas mentioned as going well included overall governance (direct (AI registry, exceptions, architecture review, refresh and currency plans) and indirect (supplier architecture review, IT strategic plans, investment business cases, procurement governance request and procurements)). For what can be done better, he discussed making governance more automated, data-driven and proactive, including by taking data from source systems and combining them together to build technical stories of each agency with application information, risk management information, PM information, and a software asset management tool to provide a complete picture that gives insight into technical debt, shows connections, and helps make informed technology decisions. Questions addressed the governance approach, what VITA seeks to accomplish through the standards, and what significant standards haven't been developed by VITA.

Cybersecurity Governance

The meeting thus far having run long, the cybersecurity governance presentation was postponed to the next meeting.

Public Comment Period

There were no public comments in-person or by email in advance of the meeting.

Other Business

Ms. Kozanas opened the floor for other business. Mr. Disney discussed travel forms and the next meeting. (Shortly after the meeting, due to scheduling conflicts, the next meeting was moved to December 11th at 1pm.)

Adjourn

The Council adjourned the meeting at 3:00pm.

VIRGINIA
IT AGENCY

State IT Governance, Modernization and Planning

Information Technology Advisory Council (ITAC)

December 11, 2024

Agenda

Governance (cont. from last meeting)	State of cyber governance
IT planning in the executive branch	COV Technology Strategy and Plan Agency IT strategic plans
Six-Year IT Modernization Plan concept and need	What should be in a 6Y IT modernization plan? Proposed ITAC roles and responsibilities

Cyber Governance

Amy Braden
Director of IT Security Governance

Authority and scope

Virginia Code § 2.2-2009 creates a scope of cybersecurity governance that is broader than VITA's core executive branch agencies: "executive, legislative, and judicial branches and independent agencies"

- But does NOT apply throughout state government, with exclusions for higher ed and authorities
- Much less visibility, from both technical and compliance perspectives, outside the executive branch

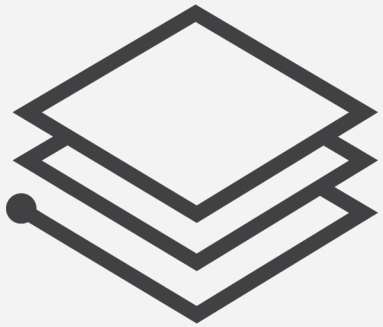
Primary objectives are to assess security risk, determine appropriate security measures and perform security audits of government electronic information.

Key policies and standards

In 2023, Cybersecurity and Risk Management (CSRM) published SEC530 a consolidation of SEC501 and SEC525 and update to the NIST 800-53

7 key policies and standards addressing cybersecurity:

- Information Security Policy (SEC519)
- Information Security Standard (SEC530)
- IT Risk Management Standard (SEC520)
- IT Security Audit Standard (SEC502)
- Security Awareness Training Standard (SEC527)
- IT Standard Use of Non-Commonwealth Computing Devices to Telework (SEC511)
- Removal of Commonwealth Data from Electronic Media Standard (SEC514)



Key deliverable guidelines and templates are available on the VITA website.

The edit and review process

- Document revision process involves collaboration and review with agency ISOs informally and formally.
- Documents are posted to ORCA* for a minimum of 30 days for non-administrative changes. If unable comply by the effective date, agencies may submit a security exception outlining that includes a plan to satisfy requirements.

CSRM shares regular updates in monthly forums such as ISOAG and ISO Council

*(*VITA's Online Review and Comment Application (ORCA) requires registration but is available to persons outside the executive branch, and even those outside state government entirely.)*

How’s it working?

Policy and standards provide Commonwealth flexibility

Policy and standard language is intentionally technology agnostic and non-prescriptive. Agency defined controls are available to accommodate agency needs.

For example, SEC530 has 244 agency defined controls. Applying broad language may be a challenge for some agencies.

Alignment with federal standards (e.g., NIST 800-53), ensures Commonwealth policies and standards meet needs of agencies with additional requirements and meets industry standards. This baseline makes it easier to assess security amid a variety of organizations.

- Federal compliance will streamline Commonwealth compliance too (e.g., FedRAMP).
- But strict federal alignment may appear more restrictive and overburdensome and not necessarily applicable at the state level.

Opportunity for improvements

- Resources permitting, CSRM could provide more standards and guidelines to meet specific needs.
- Be more prescriptive on how to meet standards.
- Provide more training to agencies on how they can leverage current policies and standards to meet their needs.
- Better agency and customer engagement as we need robust input.

What can the Committee recommend to improve?

IT Planning in the Executive Branch

Robert Osmond
Chief Information Officer of the Commonwealth

Types of technology plans in the Commonwealth

2023-2027 COV Technology Strategy

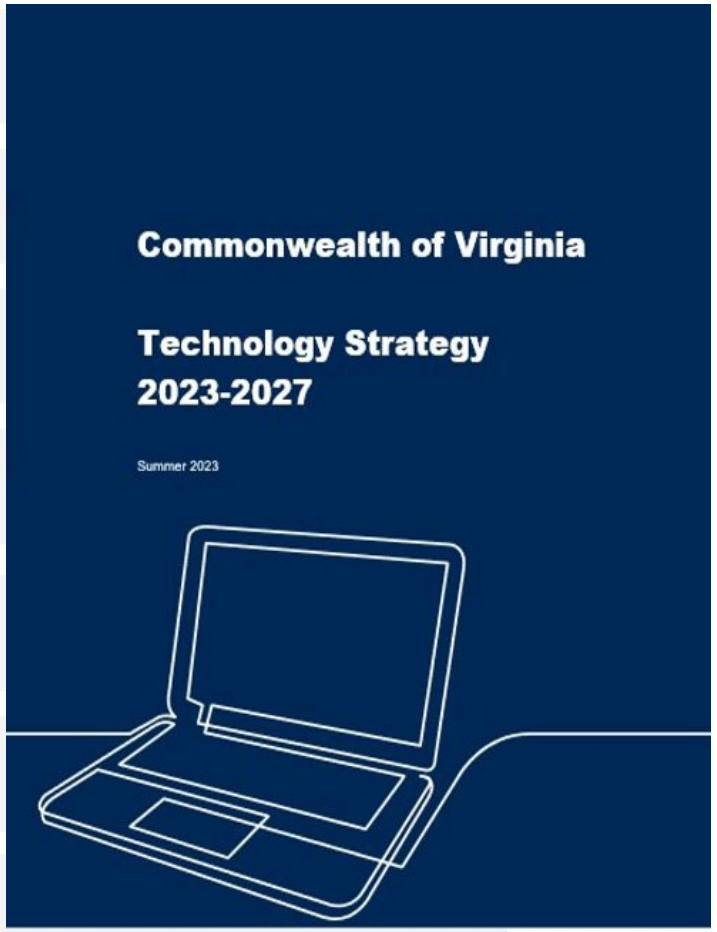
Agency IT Strategic Plans

- FY 2024-FY 2025 (current)
- FY 2026-FY 2027 (future)

- **Recommended Technology Investment Projects (RTIP) Report**

COV TECHNOLOGY STRATEGY 2023–2027

1. Transform the Virginian experience
2. Deliver with a Commonwealth mindset
3. Protect Virginians through cybersecurity
4. Drive better, faster decision-making through data
5. Advance government excellence and adaptability
6. Optimize partner ecosystem
7. Cultivate statewide IT talent capability



COV-Technology-Strategy-Summer-2023.pdf (vita.virginia.gov)

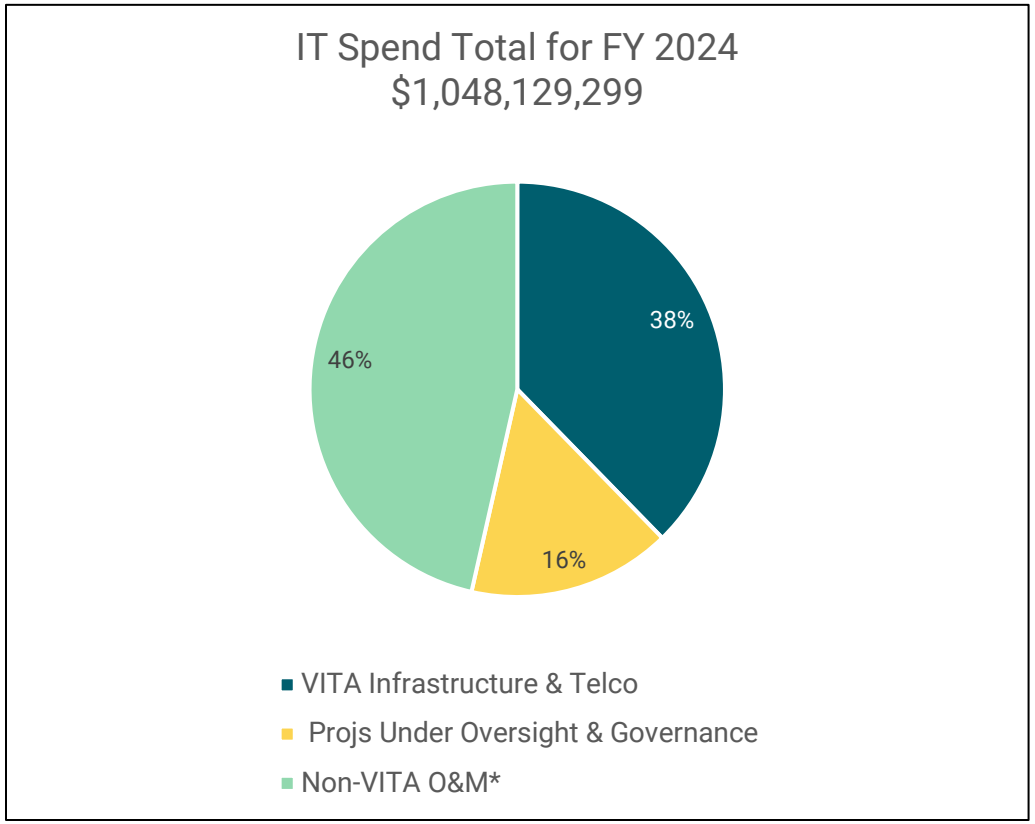
Agency IT strategic plans

IT Strategic Planning

- Each agency is required to submit an IT strategic plan (ITSP) every two years
- The plans should represent the agency's most critical technology needs for the following 1-5 years
  - Includes assessments of IT program business requirements, needed funding, staff/resourcing considerations, status of ongoing IT contracts, as well as status of aging IT systems
  - Plans are available on VITA's website
- VITA seeks to improve this process

Recommended Technology Investment Projects (RTIP) Report

- Pursuant to Virginia Code § 2.2-2007(B)(3) (as modified by Item 81(E)(1) of the 2024 Appropriation Act), the RTIP report is provided to the General Assembly annually.
- The RTIP Report consists of an overview presentation and appendices providing an overview of Commonwealth IT investments.
- RTIP reports and other IT investment and project reports are available on VITA's website.



IT spend is reported in the RTIP report

How’s it working?

What is working and improvement opportunities

What's working

- These plans are in place; the COV strategy informs both agencies and vendors; the RTIP informs the General Assembly
- Plans are becoming more fully integrated with agency business strategy (as available)
- Agency IT plans are increasingly being used to discuss agency-specific strategies and initiatives
- Agency IT plans are the primary mechanism to discuss cost control and efficiency opportunities

Improvement opportunities

- Current approaches vary by agency; mostly a reactive approach instead of proactive; too operational, not strategic
- Current plans part of VITA requirements; are sometimes seen as a box-checking/homework exercise
- Agency business/IT organization is often fractured; need continued improvement to integrate with business
- Disconnections exist between agency IT plans and agency budgets (DPB) = "December surprises"

Future state; Six-Year Planning Process

Suggested IT planning process: deductive and inductive

COV Strategic Plan

Agency IT Strategic Plan

Agency IT Budget and Recommended Investment Levels (70/20/10)

Recommended Prioritized Modernization Investments

VITA Needs Validation

Agency Needs Assessment

Agency System and Application Inventory

Deductive planning approach: strategy to investments plans

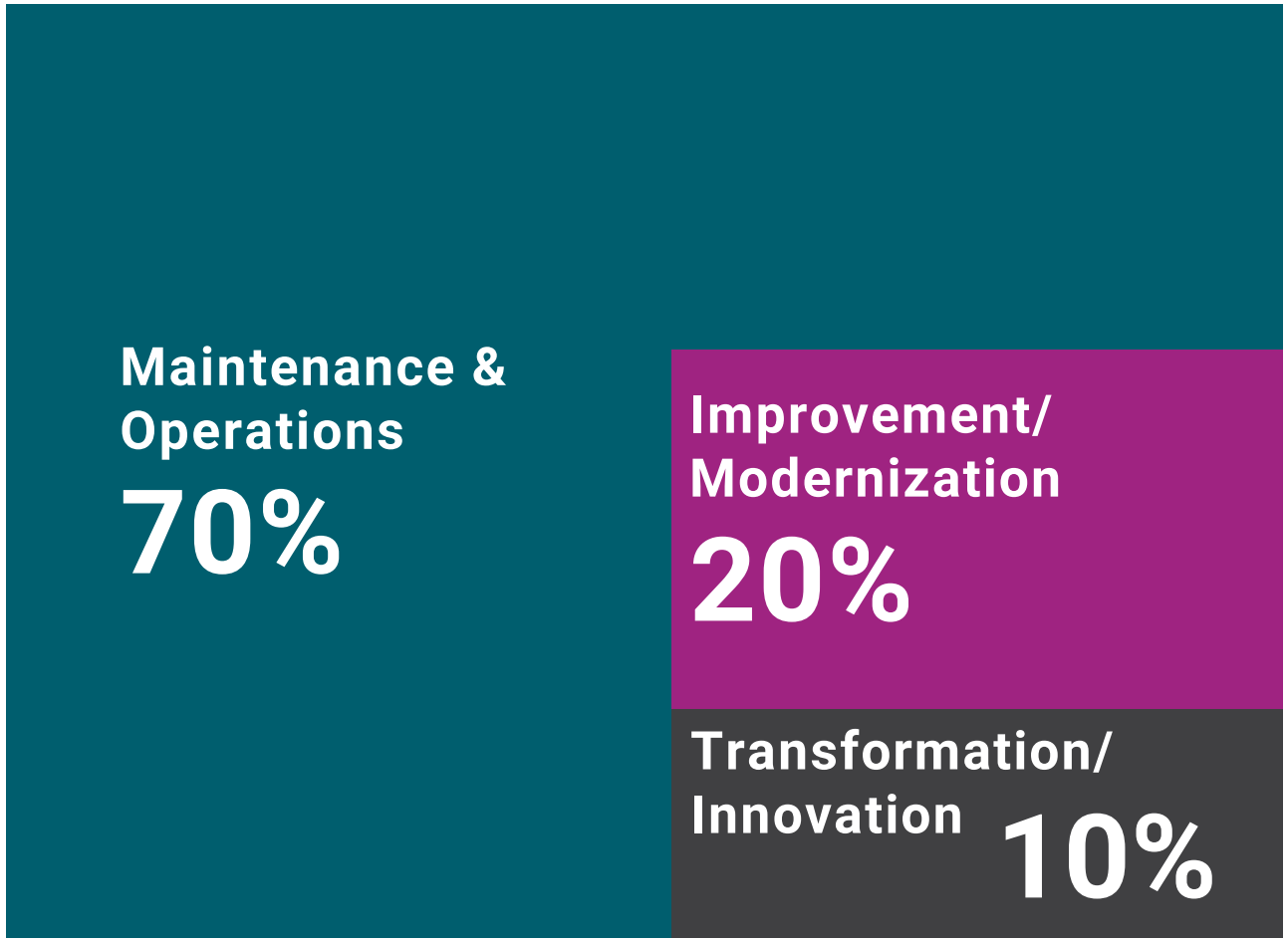
COV Strategic Plan

Agency IT Strategic Plan

Agency IT Budget and Recommended Investment Levels (70/20/10)

- Starting with the Commonwealth strategy as aligned to the agency IT strategies, validate that agency's proposed initiatives are working on the right things.
- Review the agency's overall IT budget, apply Gartner's recommended investment model, and align the agency IT budget to the agency's IT strategic initiatives (projects).

Gartner's Recommended IT Investment Levels

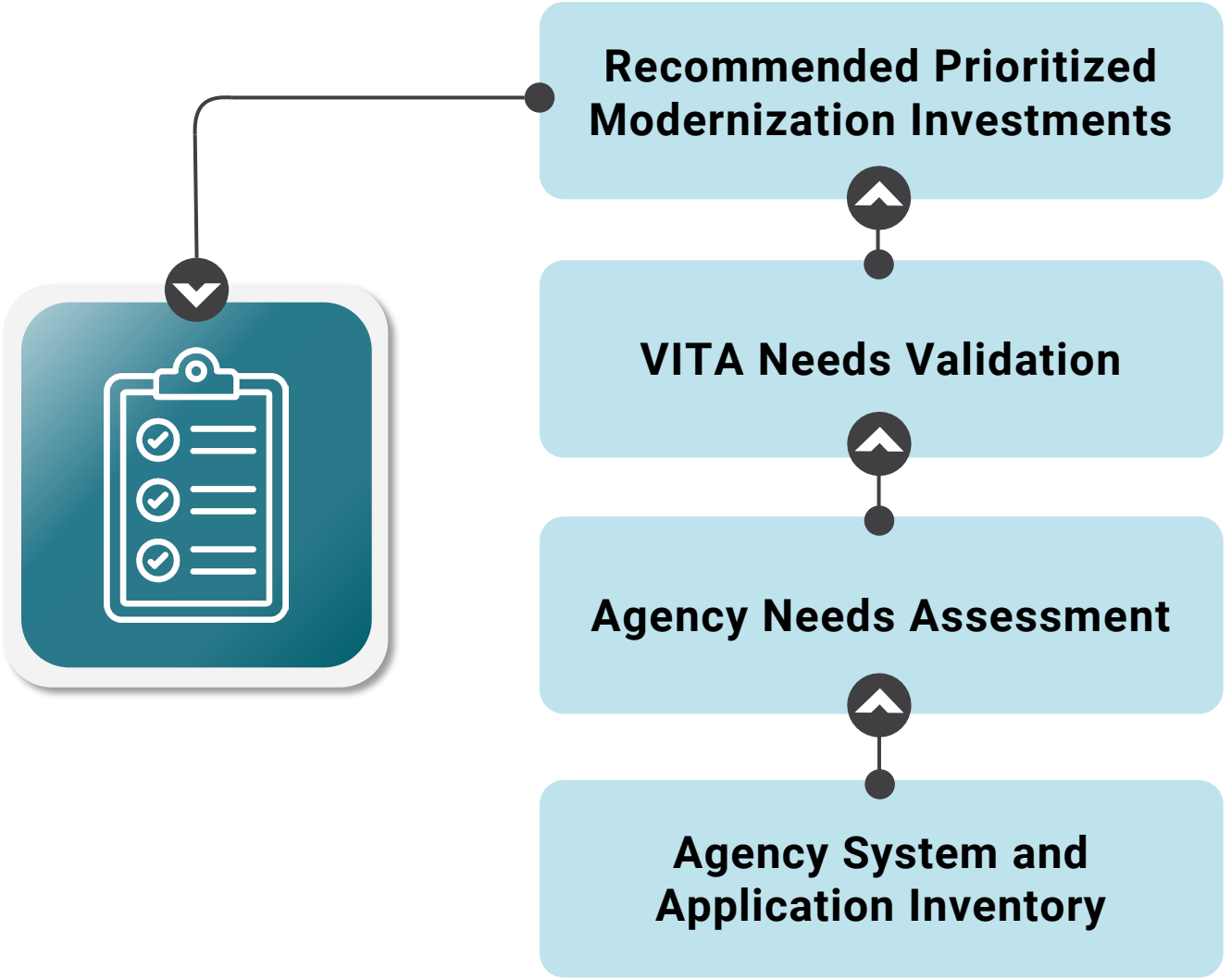


- Analysis of current total COV investments indicate an investment ratio of ~90/10 (M&O/I&T).
- Gartner's research is general, should that apply to the Commonwealth?
- Is there a better proposal for recommended investment levels?

Source: Gartner

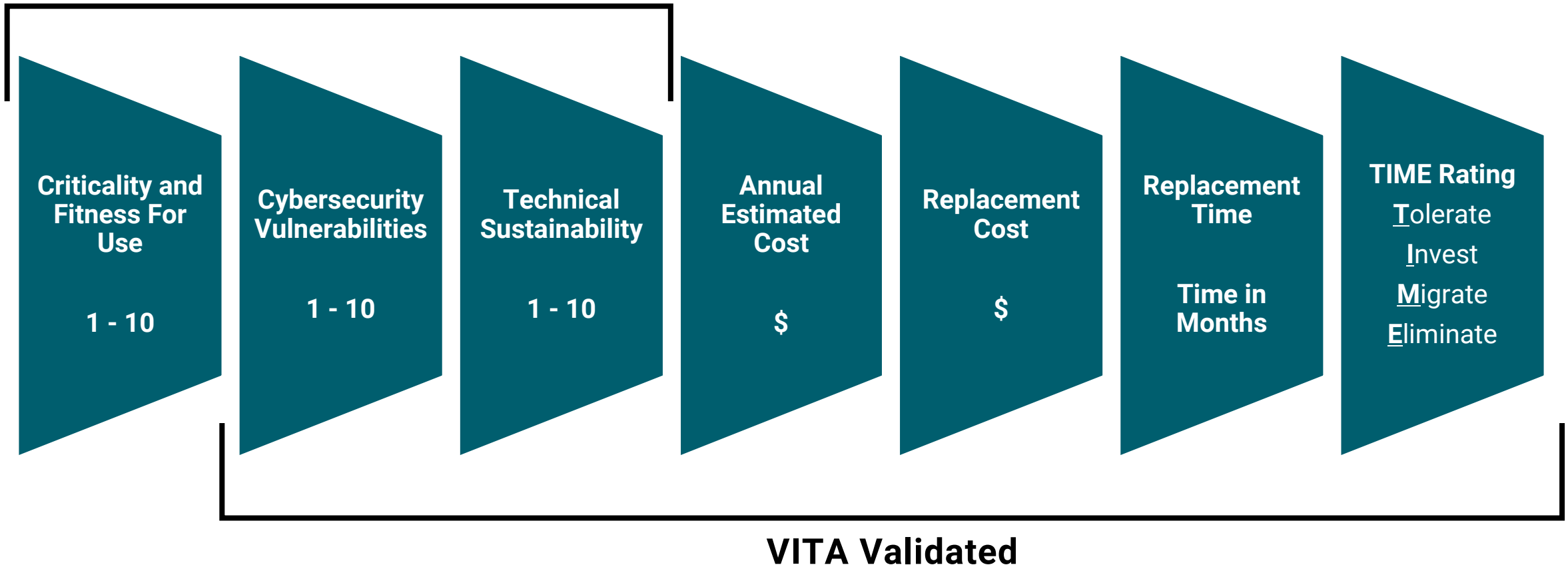
Inductive planning approach: specific needs to investment plans

- Starting with the agency's application inventory, annually rate each application to assess its overall fitness for use.
- Agencies analyze their applications and VITA validates their ratings.
- The results are scored and prioritized to determine the agency's application modernization needs.



Application Assessment Criteria - Applications Portfolio

Agency Scoring Criteria: The greater the rating, the more sustainable the application.



Application Assessment Criteria - Applications Portfolio

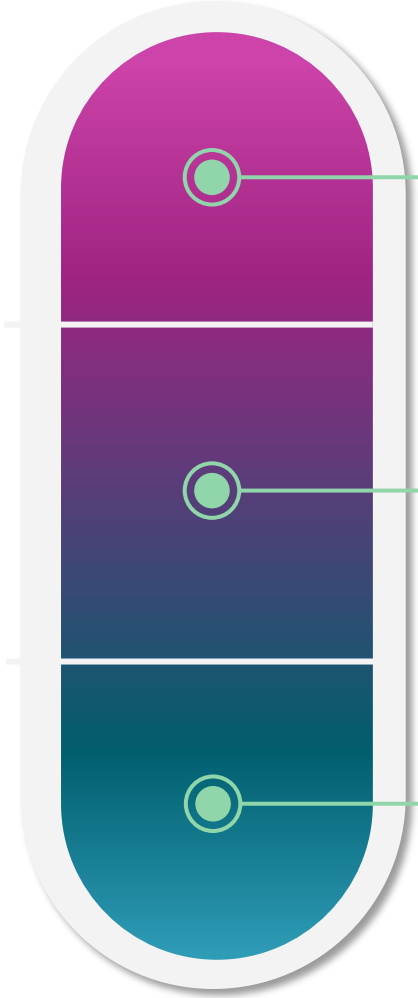
Agency Scoring Criteria

Does this scoring approach make sense? Are the categories right? Should the categories be equally rated?

- Criticality and Fitness for Use
  - 10 – Essential for agency mission and completely meets agency needs
  - 1 – Not essential and poorly meets agency needs
- Cybersecurity Vulnerabilities
  - 10 – Fully patched and no vulnerabilities
  - 5 – No critical or high vulnerabilities
  - 1 – Critical and high vulnerabilities that can't be addressed
- Technical Sustainability
  - 10 – On long-term sustainable technology
  - 1 – Out of support technology

Core Application Assessment Scoring

- The rating approach is multiplicative (10*10*10) for a max score of 1000 and a min of 1. The lower the score, the more acute the modernization need.
- The team suggested a notional scoring approach as an initial approach. Is there a better way?



Acute need
1-250

Impending need
251-500

Maintain
500+

* End result: 1 to n list of applications with highest risk at #1

Developing the Six-Year IT Modernization Plan

		VITA Risk Low – 8 Medium – 5 High - 2	VITA EA Low – 8 Medium – 5 High - 2	Replacement Cost	Time
Application	Criticality & Fit for Use 1-10	Cybersecurity Vulnerabilities 1-10	Technology Sustainment 1-10	Annual Estimated Cost	
				$1,000	
		1-250 Acute		$100,000	
		251-500 Improving		$500,000	
		500+ Maintain		$1,000,000	
		Agency Budget = 70/20/10		$2,500,000	
				$5,000,000	

Example: VITA Telecom Billing System: Criticality and fitness for use (5 for statewide use and generally functional), cybersecurity vulnerabilities (8 for no critical or high vulnerabilities), technology sustainment (2 for end of life and support) = 80 (acute need: replacement project called TEMS underway to address).

Knowing year 1 investment levels and needs...planning for 6 years

COV Strategic Plan

Agency IT Strategic Plan

Agency IT Budget and Recommended Investment Levels (70/20/10)

Recommended Prioritized Modernization Investments

VITA Needs Validation

Agency Needs Assessment

Agency System and Application Inventory

The reasons for a six-year IT modernization plan

What decisions are needed?

- IT funding levels at both the Commonwealth and agency level(s).
  - Administration budget request
  - General Assembly budget approval
- Approval for significant discrete IT project investment funding requests.
- Commonwealth and agency directives to sufficiently prioritize IT portfolio maintenance and investments.
- Executive and legislative actions direct technology execution.
- What other decisions need to be made?

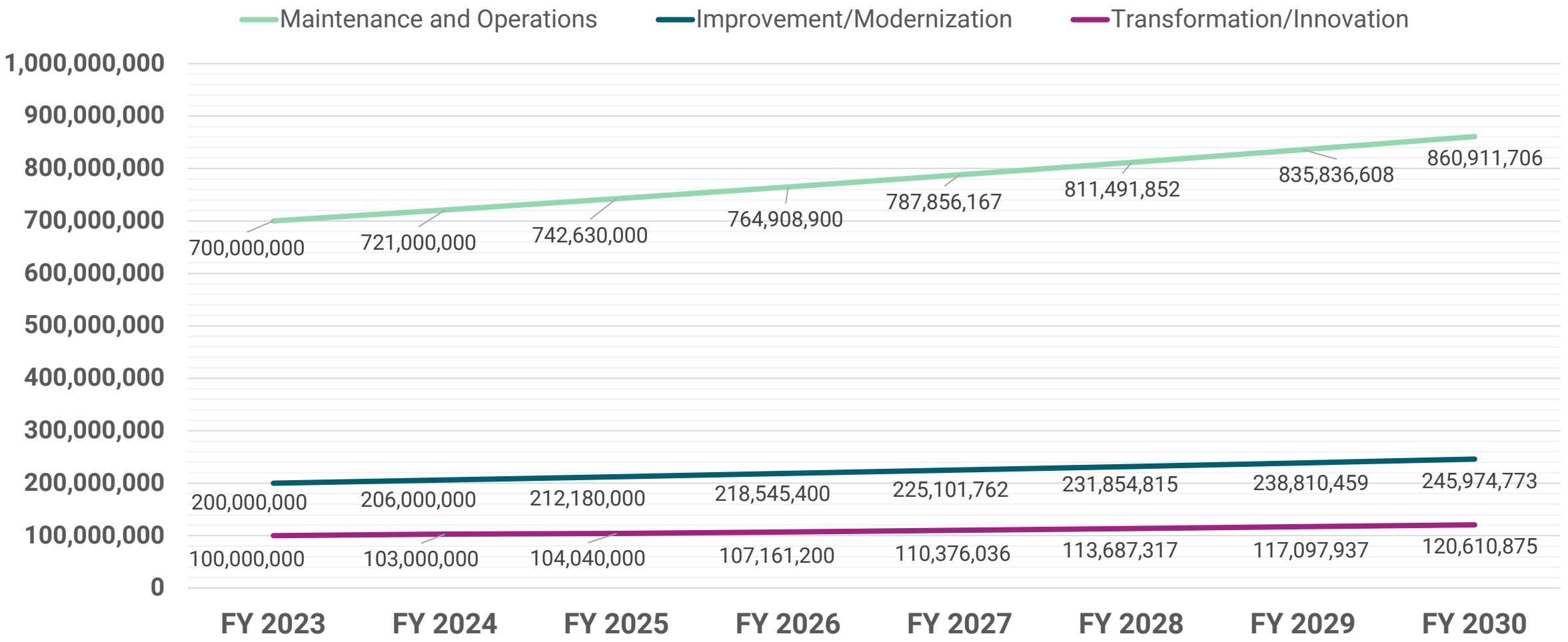
What information is needed to decide?

- Current and expected future IT funding requirements.
- Current multiyear IT project funding obligations based on approved projects in the IT portfolio (proposed and active).
- Potential budgetary space for IT projects in future years.
- Backlog of technical debt based on the application needs assessment.
- What other information would be needed?

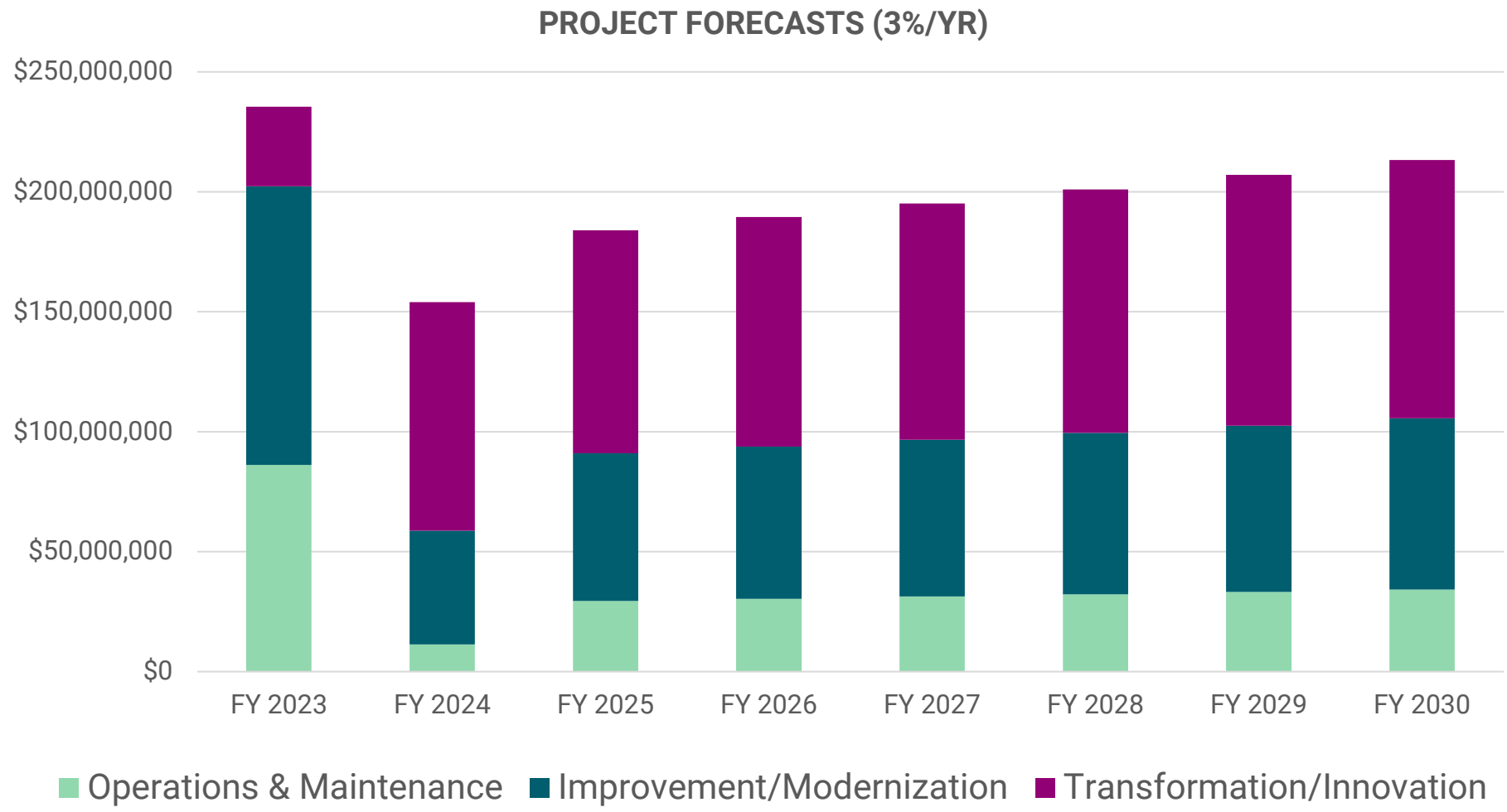
Example 1: IT Six-Year Planning Scenario

Starting Total: $1B
Assumption: 3% increases year over year

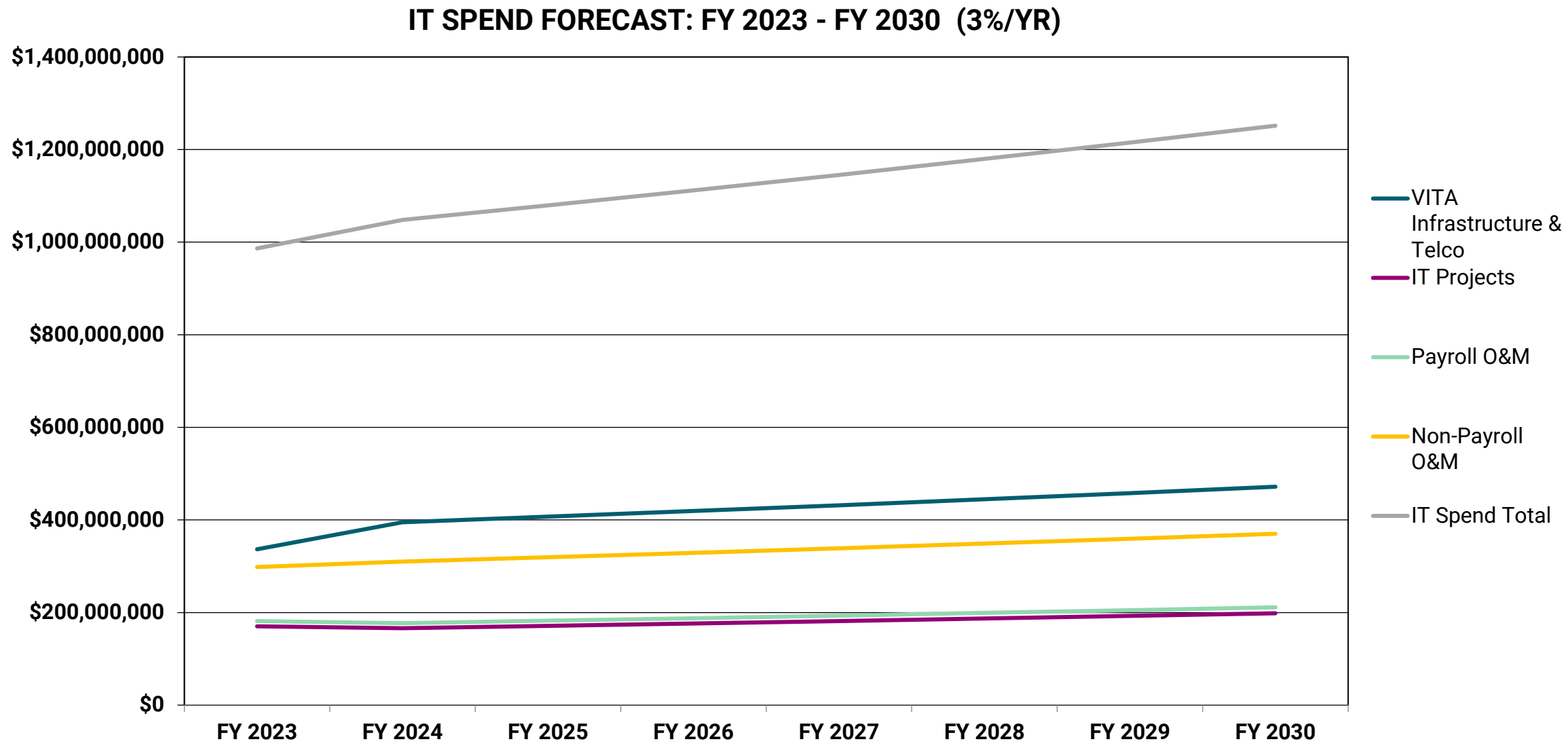
Budget makeup - estimate



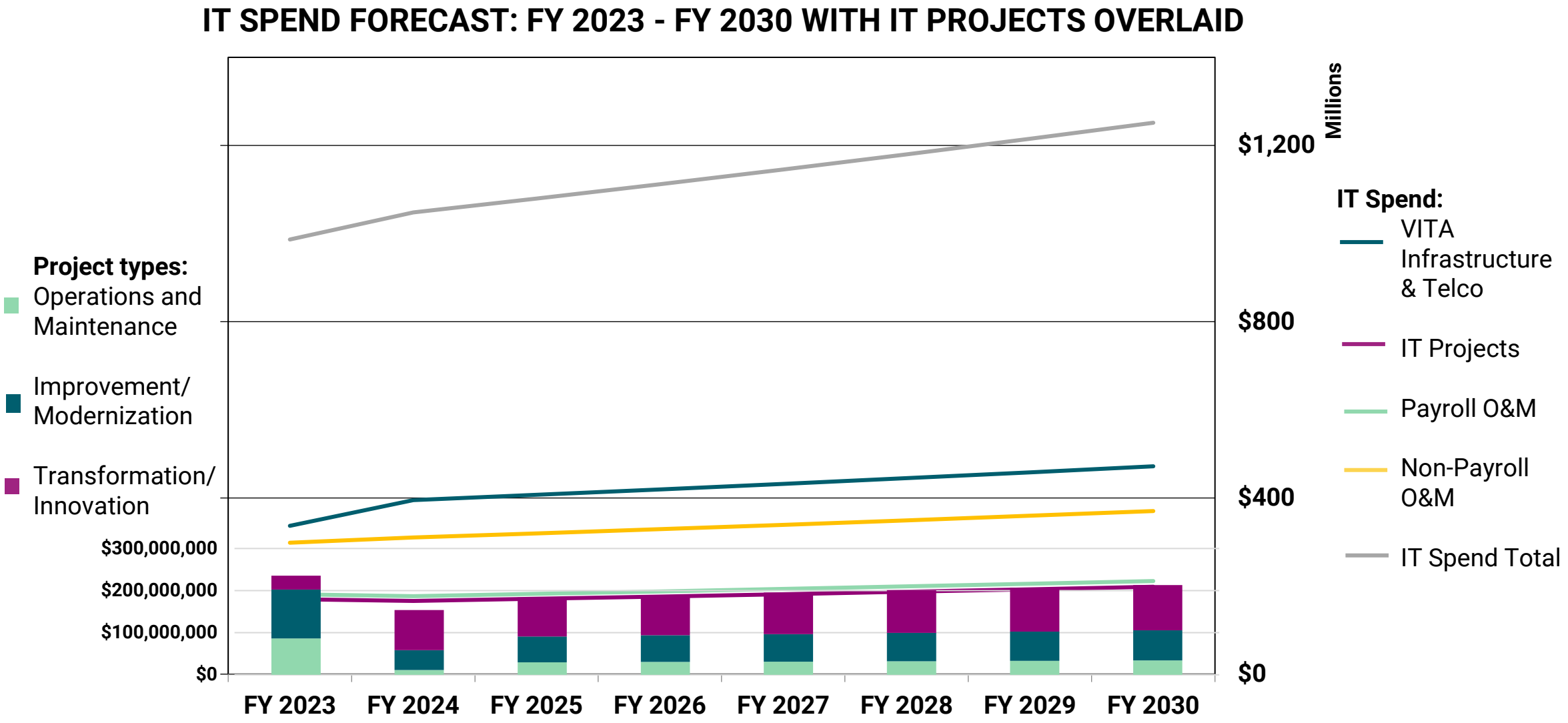
Example 2: Six-Year IT Projects Planning Scenario



Example 3: Six-Year IT Category Spend Scenario



Example 4: Six-Year IT Plan Summary



Proposed role for ITAC

- **What is the proposed ITAC role within the Six-Year planning process?**

- **Alignment with ITAC roles in Va. Code § 2.2-2699.6:**

  3. Advise the CIO on strategies and priorities for information technology for executive branch agencies;
  4. Advise the CIO on information technology planning and projects;
  5. Advise the CIO on policies, standards, and guidelines for information technology and data of the Commonwealth; and
  6. Advise the CIO on information technology budgeting, investments, and expenditures.

Questions and discussion

Thank you