2024 INFORMATION TECHNOLOGY STRATEGIC ASSET MANAGEMENT PLAN

For Information Technology

The Information Technology Strategic Asset Management Plan (IT SAMP) documents the information technology assets hosted in the Bonneville User Domain (BUD) and cloud-based services. The IT assets hosted in the BUD provide the network connectivity (both voice and data), computational resources, and automated business solutions that enable Bonneville Power Administration (BPA) staff to securely and reliably perform their business functions on a daily basis. The plan also examines IT's current state of maturity in asset management relating to people, processes, and systems, and offers a path forward to asset management improvement to ensure maximum value is derived from IT assets.

Table of Contents

1.0 EXECUTIVE SUMMARY

Bonneville Power Administration's (BPA) Information Technology (IT) organization, products, and services fill a key role in facilitating the high-reliability of the BPA transmission system and enable the full spectrum of BPA business activities. The services they provide have a profound impact on the effectiveness and efficiency of BPA's processes and people. The Information Technology Strategic Asset Management Plan (IT SAMP) is intended to provide the lifecycle planning and execution strategies to enhance cyber security, strengthen resource stewardship, and maximize the value of IT assets while minimizing risk. The IT SAMP provides clear alignment with the BPA Strategic Plan, organizational objectives, and business requirements. The resulting asset management objectives ensure that IT assets are managed and measured to create and deliver value to BPA. The underlying structure and discipline of Institute of Asset Management (IAM) tenets and principles play a key role in the maturation and success of IT asset management.

Some significant changes since the previous IT SAMP include:

- Issues related to IT hiring:
  - Low supply and high demand in the IT job market are driving higher costs of IT labor, increasing budget pressure for both supplemental labor and federal positions. Federal wages are unable to keep pace with commercial offerings, driving the need to use retention programs to attact and retain suitable employees and driving up the cost of labor.
  - The pandemic has demonstrated the ability of the IT workforce to effectively work remotely, driving newhire demands for remote work support, and hampering IT hiring that does not yet support it.
- Cyber security threats continue to rise on a global basis, driving the need to strengthen cyber security posture throughout the utility industry, and to meet added cyber security requirements from DOE, OMB, DHS, WECC and others. Paramount is the notion of Zero Trust Architecture. While not yet fully mature, it entails a radical change in cyber security practice and philosophy that will likely require a re-structuring of all networks and service delivery that promises to drive significant effort and cost for years to come.
- A better understanding of the requirements to achieve desried levels of asset management maturity has driven a lower assessment of current IT capabilities in this area, and helped to identify needed improvements.
- Recognition by executive management that constrained budgets have resulted in underfunding IT work to the point of impacting business line program delivery.

IT program development in the areas of asset information, decision making and asset management competencies shape the SAMP strategies to improve on the current state. To achieve the future state, IT needs to mature its asset management practice to implement and use a robust set of health monitors (see Section 8) for information not only on asset performance, but to include information on how well the asset is achieving business needs and the financial efficiency of the asset relative to other alternatives. IT needs to partner with business units to ensure assets are delivering more business value than the cost of maintaining the assets by monitoring both business value and operational costs. When the business value begins to drop, IT (in partnership with the business) must determine the appropriate corrective action (i.e., upgrade, enhancement, replacement, or retirement) and update asset plans which may be used to inform future IT SAMP and budget processes.

In addition to sound asset management execution, the IT SAMP addresses significant external and internal influences facing IT in terms of supporting an electric utility while also being a Federal element of the Department of Energy. These influences create a number of challenges for IT at BPA, which can be grouped into the following categories: Federal Statute Compliance (with cyber security at the forefront), IT Technological and Budgetary Challenges, and Strategic Partnerships with BPA business lines to identify and resolve customer demand for efficiencies driven by automation.

IT costs continue to rise from economic inflation, additional volume usage of existing assets, rising compliance requirements, and new customer demand for additional business capabilities. IT has no choice other than to plan and execute programs for IT business improvements to support business line strategic initiatives that will drive BPA to successfully meet its mission. After several years of holding expense funding as low as possible, IT has reached a state where nearly all IT effort must focus on maintaining existing systems, which is curtailing IT's ability to meet new customer demand. This has resulted not only in lower asset performance (more system outages), but created a long list of both work efforts to regain acceptable health levels and a growing backlog of pent-up customer demand. IT will need both capital and expense funding adequate to maintain existing systems (Sustain) and to support business line strategies for advancing the BPA mission (Expand). Right-sizing IT staff to adequately meet these goals is imperative for success.

Some of the new systems and capabilities driving the need to increase expand funding include:

- Integrated Contract Lifecycle Management
- Outdoor Ballistic Detection
- Rapidly Deployable Security Systems
- Continuity and Disaser Recovery
- Fleet Telematics
- Day Ahead Market
- WRAP
- Computerized Maintenance Management
- Wildfire Management
- Zero Trust Architecture
- Transmission Asset Portfolio Optimization Tool

These also create additional increases in core operations and maintenance budget requirement after project implementation and the costs must be identified and included in core budgets, and in fact are identified in the future spending forecasts contained in the tables in section 10 (Expense for O&M Tail, average of 8.2% of implementation cost).

2.0 ACKNOWLEDGEMENTS

2.1 Senior ownership

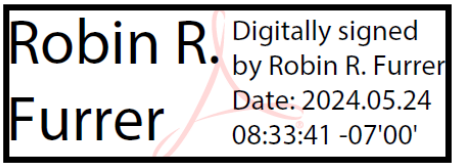
Secure and reliable automation of business needs and work processes, through Information Technology (IT), is a key enabler for Bonneville Power Administration in delivering low cost and reliable power for the region.

In support of automating business needs and achieving BPA strategic objectives, IT is committed to:

- Enable BPA to reliably and securely use IT resources to effectively and efficiently perform work while maximizing utilization of IT resources.
- Optimize total cost of ownership by balancing the costs of new investments for upgrades and replacements with operations and maintenance (O&M) costs.
- Balance individual BPA lines of business immediate requirements with BPA strategic objectives by delivering flexible and extensible assets that meet current objectives and can be leveraged to meet future strategic business objectives, resulting in reduced future delivery times and least total cost of ownership.
- Securely maintain and operate assets in accordance with federal and industry regulations and laws.
- Institutionalize Operational Excellence through the adoption of maturity models for continuous measurable improvement of processes, practices, and service delivery, maximizing the value of our IT assets and reducing the cost of O&M.
- Become a strategic partner, advising and assisting business lines and BPA in leveraging technology to meet and achieve our objectives, collaborating with our business line partners to understand and meet their business goals.

This IT Strategic Asset Management Plan represents a continuation in achieving these commitments. Given the rapid changes in IT and the need to provide greater business value at lower costs, BPA's Enterprise IT must accelerate its adoption of technology and leading industry practices to achieve cost efficiencies.

I am committed to the improvement of our IT program through the development of asset management competencies and fundamentals. We see opportunity to make informed investments in our assets in order to rationally respond to the real challenges presented by continued constraints in labor and expense funding. I am confident that our active collaboration with our business partners and our attention to asset management principles will allow us to meet these challenges with transparency and a deeper understanding of business impacts.



Robin Furrer

Chief Administrative Officer

2.2 Strategy Development Approach

IT continues to work on maturing asset management practices. This includes building processes that will lead to maintenance and evolution of our Strategic Asset Management Plan that incorporate updates and changes in asset plans, IT strategy, and business strategies. Figure 2.2-1 shows the annual cycle that we have been building. A few key features include:

- Business input directly from clients and BPA's strategy – these touch points are still developing and have advanced through the assignment of IT Strategic Business Partners to Power, Transmission, and Corporate lines of business.
- Updates to the IT technical architecture are reflected in the various IT asset portfolios (Datacenter, Network, Office Automation, and Applications) – this touch point is maturing, although slower than anticipated due to staffing reductions.
- All these updates are reflected in the IT SAMP and the IT SAMP influences strategies, asset plans, and funding levels.

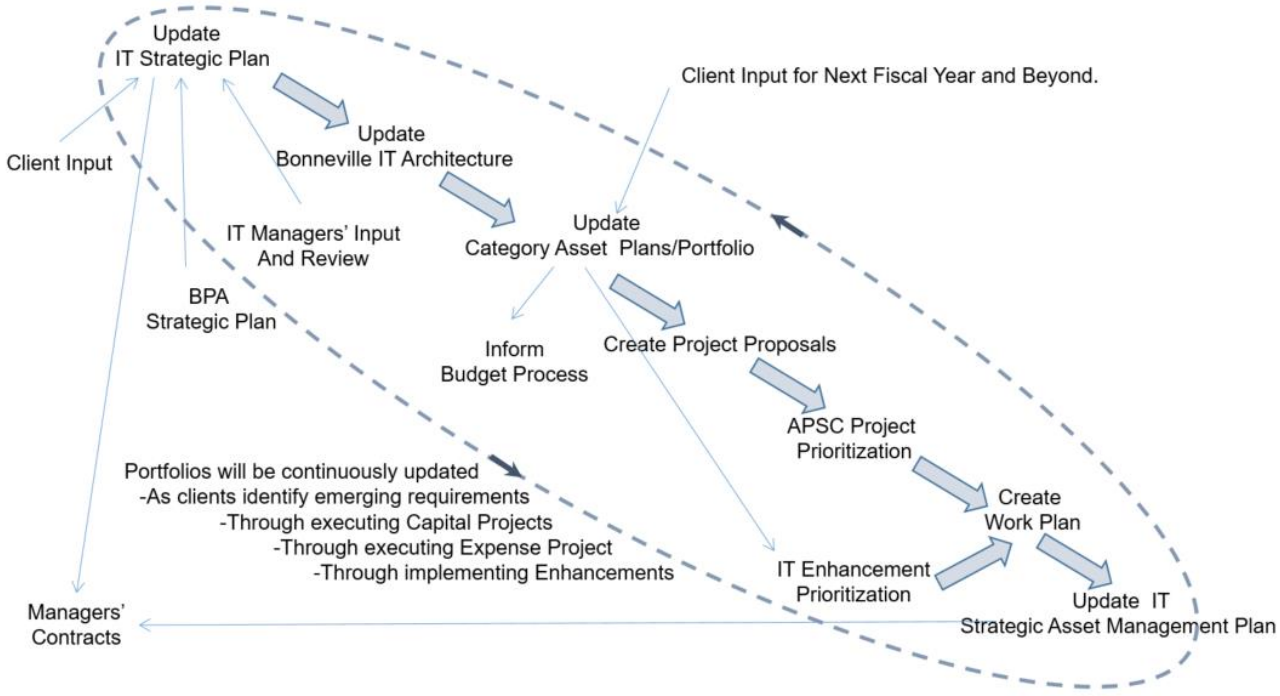


Figure 2.2-1 Annual Asset Management Cycle

2.2.1 Key Contributors

The IT Asset Manager coordinates and develops the IT Strategic Asset Management Plan. To deliver the IT SAMP, the IT Asset Manager coordinates with the following:

- Management of the three major business lines - working through the IT Strategic Business Partners.
- Chief Information Officer – sets direction and goals for BPA Information Technology services and ensures business needs are prioritized and addressed.
- Chief Administrative Officer – who validates IT direction and goals for service delivery and ensures the IT SAMP sets the proper tone.
- IT Tier-2 Organizational Managers
    - Manager, Office of the CIO
    - Manager, Cyber Security
    - Manager, Critical Business Systems Operations and Development
    - Manager, Entgerprise Shared Services
    - Manager, Enterprise Technology Operations Services
- Category Asset Managers – managers responsible for maintaining the Datacenter, Network, Office Automation, and Application asset plans (there are nine IT category asset managers).
- System Owners (SOs) – managers that maintain an application (asset) and coordinate with Information Owners (business user) on activities to maintain, enhance, and/or replace assets.
- Project Management Office (PMO) Manager – manages the PMO while facilitating the Agency Prioritization Steering Committee (APSC) and makes recommendations to the CIO for project prioritization investments that deliver new assets into production, upgrades existing assets, or replaces/retires assets.
- Strategic Planning/Business Transformation Office – provides documentation on BPA's Key Strategic Initiatives, and leads the BPA effort for Enterprise Architecture.

2.2.2 Key Activities

Figure 2.2-1 depicts the major ongoing activities that maintain the information needed to develop and maintain the IT Strategic Asset Management Plan. These activities include the following:

- Use BPA, business, and IT strategic plans/roadmaps to update IT asset plans.
- Review asset plans to:
    - Ensure plans reflect BPA, business, and technology roadmaps
    - Assess asset health indicators
- Review newly implemented asset health indicators (see section 8 for details) to determine if underlying systemic issues need to be addressed by the IT SAMP.
    - IT is at a low level of maturity in maintaining and using health indicators to determine overall health of application assets.

- Financial metric health indicators are at too low of a maturity level to provide reliable insight on application asset condition to determine if an asset is meeting financial performance objectives or needs an investment to either restore business value or replace the asset.
- Use IT asset plans to inform/update the IT SAMP and vice versa.
- Develop funding levels based on refresh rates and assessment of impact of business roadmaps.
  - With current level of maturity of business roadmaps, IT is unable to determine yearly projections of future capital needs with much certainty.
  - Expense funding levels were developed using a combination of historical costs and expected new expense costs from new application assets being delivered into production.
  - Expense funding considers if future projects will result in cloud-based solutions which require higher levels of expense than capital.
- Vetting the IT SAMP with key contributors.
- Ensuring asset plans are updated to align with the final FY2024 IT SAMP.

3.0 STRATEGIC BUSINESS CONTEXT

3.1 Alignment of SAMP with Agency Strategic Plan

For many years, BPA's vision has been to be an engine of the Northwest's economic prosperity and environmental sustainability through delivery of safe, reliable, and resilient power and transmission operations, providing power for what it costs to produce and protecting local natural resources and enhancing conditions for fish and wildlife. In support of this continuing vision, BPA released its 2024-2028 Strategic Plan.

The direction of BPA's Strategic Plan has set forth goals which will sustain and further BPA's mission and vision.

To champion these strategic goals, Information Technology outlines key objectives in the IT SAMP which are centered around these goals. IT's achievable objectives maximize the value of the existing IT assets while mitigating the reliability and compliance risks to the program posed by an ever-changing portfolio. This establishes the framework used to align our next several years of investments and strategies with these four Agency strategic goals:

- Enhance the value of products and services
- Mature Asset Management

- Preserve safe, reliable system operations
- Modernize Business Systems and Processes

The guidance defined in the IT SAMP establishes the specific high-level strategies required to inform the development of the more tactical IT Asset Plan (AP) and support the delivery of the Agency strategic goals and objectives.

The IT SAMP focuses on four asset management objectives, which are aligned with the BPA Strategic Plan as follows:

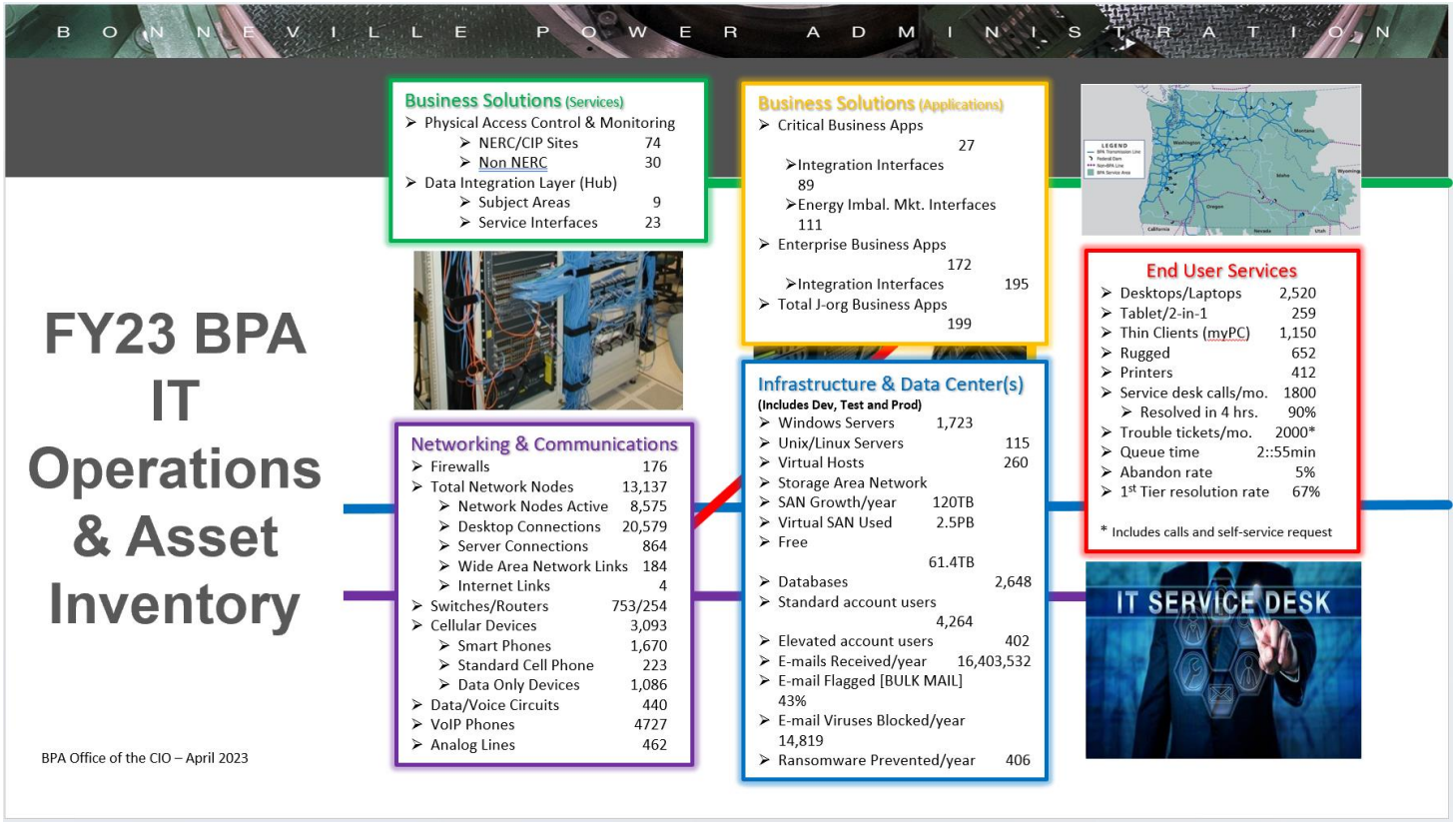
- **IT Asset Management Objective 1: Improve IT asset data management and asset planning**
  - A) Invest in systems and documented processes to better define, collect, store and analyze IT asset data in support of data-based decision making. This initiative will aide with determining criticality, health, and risk profiles and prioritization of IT asset life cycle activities.
  - B) Improve joint business and IT planning for technology strategic needs to make improvements in planning for specific solutions and collaborative development of Strategic Asset Management Plans and Asset Plans, leading to integration with business goals and plans, and increasing the efficiency and effectiveness of IT projects.
- **IT Asset Management Objective 2: Support emerging agency business needs**
  - A) Application of existing or acquisition of new IT automation assets to facilitate business efficiency capabilities in support of new market opportunities (e.g., Energy Imbalance Market, corporate systems modernization, and other executive initiatives).
  - B) Integrate focused investment strategies in IT infrastructure which are risk informed, cost effective, realistic, and scalable in order to deliver and maintain IT automation in alignment with business requirements.
- **IT Asset Management Objective 3: Expand resilient business processes**
  - A) Invest in additional operational and cyber security monitoring to identify emerging threats and pro-actively mitigate issues.
  - B) Build out additional geographically dispersed continuity of opertations (COOP) capabilities to improve business resiliency.
  - C) Assign higher priority to compliance initiatives to meet federal security standards and other regulatory requirements, improving reliability and risk management.
- **IT Asset Management Objective 4: Focus on IT asset service delivery**
  - A) Implement industry best practices, such as Information Technology Infrastructure Library (ITIL) or IT Service Management (ITIL), to improve visibility into the cost of IT services, centrally manage customer demand for IT services, and focus available resources on the highest value work.
  - B) Develop methods to maximize reuse of existing assets, steadily reduce technical debt, and promote a culture of innovation to maintain a modern technical architecture right-sized to support the mission.

Table 3.1-1, SAMP Alignment with BPA Strategic Goals

BPA Strategic Goals	IT Objective 1 (Value)	IT Objective 2 (Reliability)	IT Objective 3 (Reliability)	IT Objective 4 (Reliability)
1. Invest in People				
2. Enhance the Value of Products and Services **Objective** 2.2 Foster market evolution across the West to enhance the delivery of cost-effective and reliable service. **Outcome** 2.2.3.	X			
3. Sustain Financial Strength				
4. Mature Asset Management **Objective** 4.1 Improve asset management data and system capabilities. **Outcome** 4.1.1 **Objective** 4.2 Enhance risk-based decision-making and portfolio optimization. **Outcome** 4.2.1 – 4.2.4.		X		
5. Preserve Safe and Reliable System Operations **Objective** 5.2 Strengthen resilience in preparation for high-impact events and system change. **Outcome** 5.2.1, 5.2.4 **Objective** 5.3 Advance a culture of compliance to meet changing requirements, improve reliability and manage risk. **Outcome** 5.3.1	X		X	
6. Modernize Business Systems & Processes **Objective** 6.1 Develop more cost-effective, well-organized, and efficient systems for managing technology and business operations. **Outcome** 6.1.1 – 6.1.10 **Objective** 6.2 Strengthen the resiliency and security of information and operational technology. **Outcome** 6.2.1 – 6.2.3			X	X

3.2 Scope

The Information Technology Strategic Asset Management Plan covers the information technology assets hosted in the Bonneville User Domain (BUD) and cloud-based services. The IT assets hosted in the BUD provide the network connectivity (both voice and data), computational resources, and automated business solutions that enable BPA staff to securely and reliably perform their business functions on a daily basis. Common aspects of these physical and virtual assets include network switches/routers and cabling plants, network circuits, wireless access points, servers, data/file storage, laptops, workstations, thin clients, printers, monitors, smart phones, desktop and back-office applications, specialized business applications, etc.



The IT SAMP does not cover information technology assets identified as Operational Technology (OT). In this context, Operational Technology (OT) is the hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events for operation of BPA's electric grid. The BPA Chief Information Officer (CIO) exercises oversight through his managers and a close relationship with the director of Transmission Technology (TT-org). The director of TT is responsible for managing information technology assets identified as OT. These OT assets are documented in Transmission's SAMP.

IT also shares responsibility with BPA's physical security organizations for the provisioning of security devices such as surveillance cameras and card readers, and monitoring stations. Typically, the hardware is provided by the physical security organizations and therefore not included in the IT SAMP, but maintenance of that equipment does fall to IT.

3.3 Asset Description and Delivered Services

The IT asset category is divided into four major portfolios: Office Automation, Network, Data Center, and Applications. The physical infrastructure components of the first three IT asset portfolios are straightforward: they provide the physical means by which people connect to the machines that enable workers to carry out their daiy functions. The Applications portfolio includes critical business systems and general business systems, as well as small single task-related applications specific to certain job functions. Critical business systems must be available 24 hours by 7 days per week in support of hydro operations, fish operations, and power revenue generation. Enterprise business systems enable BPA to manage staff, finances, facilities, supply chain, transmission assets, and services such as managing circuits and work planning. As a whole, Information Technology assets provide the foundational capabilities that enable all other asset categories and business functions to effectively and efficiently meet their missions.

Table 3.3-1, Assets

Portfolio	Assets	Activities
Office Automation	Support for workstations, laptops, tablets, printers, productivity software, peripherals (scanners, portable hard drives, etc.), smartphones, cameras, monitors, projectors, and large format displays throughout BPA's service territory	○ Maintain network printers and desktops/laptops and peripherals in accordance with the asset life cycles ○ Upgrading misc. productivity software ○ Adoption of new technologies ○ Obtaining/ensuring compliance with architectural standards and security controls
Data Center	Servers (infrastructure servers, application servers, database, etc.) operating systems, database management systems, and management tools	○ Maintain servers and storage in accordance with the asset life cycles ○ Migrating to new server operating systems ○ Adopting new technologies (virtual storage, server virtualization, cloud services, etc.) ○ Enhancement of data center (improving bandwidth, improving backup and recovery, server consolidation, etc.) ○ Obtaining/ensuring compliance with architectural standards and security controls
Network	Data, voice, and video networks. Includes fiber and cable plant, switches, routers, firewalls, web filters, Domain Name System Security Extensions (DNSSEC), Intrusion Detection and Intrusion Prevention Systems (IDS/IPS), Virtual Private Networking systems (VNP), management and security software, designing, procuring and implementing circuits and BPA's Multiprotocol Label Switching (MPLS) cloud (including monthly bill audits and payments), video teleconferencing (VTC) and Voice Over IP (VoIP) (including dispatch telephone system, broker boxes and recording system)	○ Maintain network infrastructure (routers, switches, hubs, firewalls, cabling, etc.) in accordance with the asset life cycles ○ Enhancement of network infrastructure (remote access, wireless access, etc.) ○ Adoption of new technologies (tele-presence, messaging convergence, Internet Protocol version 6 (IPv6), etc.) ○ Obtaining/ensuring compliance with architectural standards ○ Enhancements/modifications to meet emerging security threats

Portfolio	Assets	Activities
Applications	Applications are split into two sub-portfolios: Critical Business Systems (CBS) and General Business Systems(GBS); Critical Business System (CBS) require 24x7 availability and support: • Real time or preschedule transmission or power scheduling • Hydro operations • Marketing (deal capture, day ahead trading) • Short term forecasting, planning and loads There are approximately 20 critical business systems. General Business Systems support the administrative tasks, asset management, long term planning and forecasting, contracting, human resources, purchasing, and financial management. There are over 200 general business systems.	○ Proposals for delivering new functionality ○ Upgrades and/or enhancements (typically expense) ○ Software-as-a-Service (SaaS) ○ Applying system or security patches ○ Implementing new features to meet business needs ○ Correcting bugs or erroneous computing conditions ○ Implementing annual changes such as tax code changes ○ Retirement and/or disposition of systems ○ Maintaining systems in compliance with the enterprise architecture and security controls

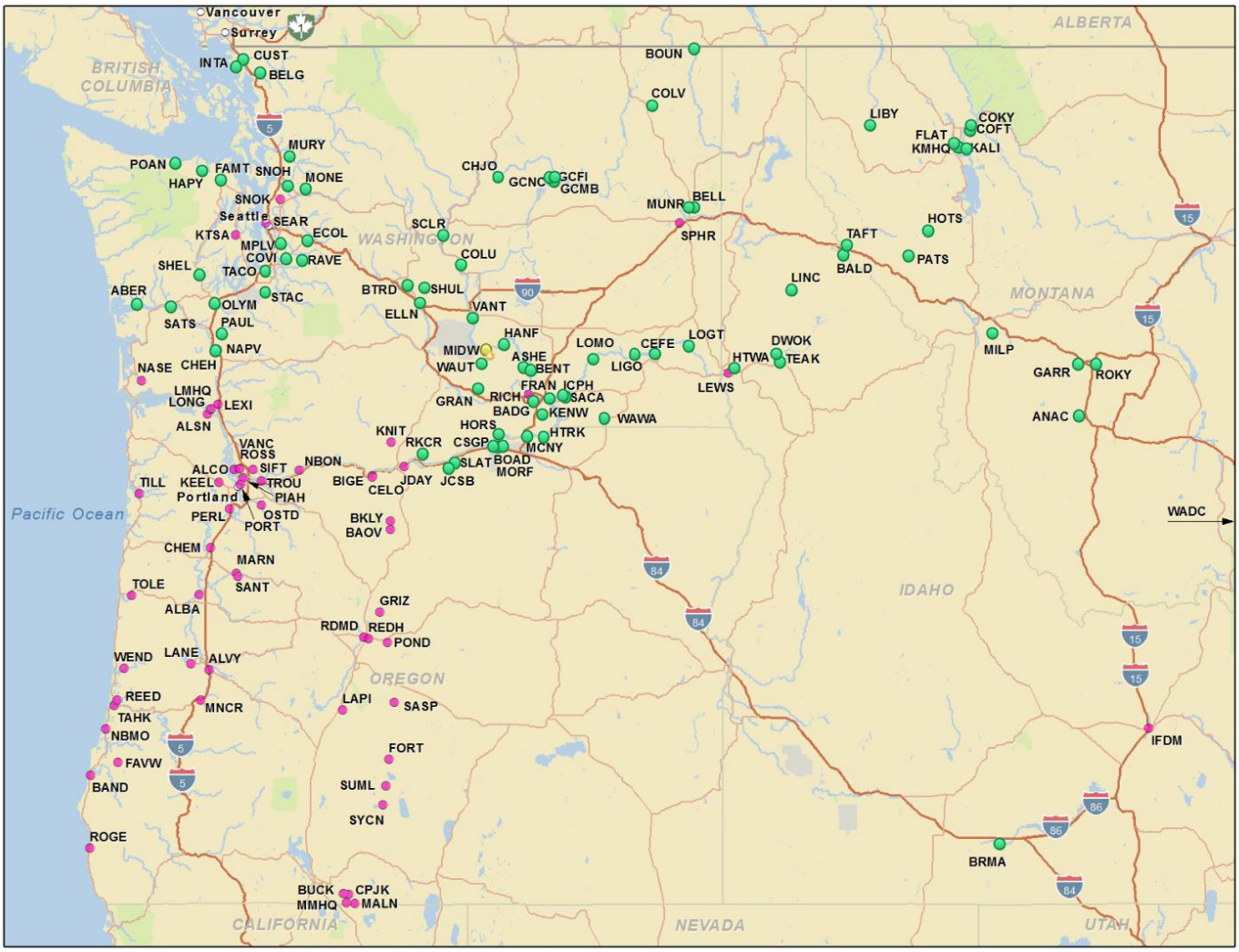


Figure 3.3-2, Asset Locations

Figure 3.3-2 shows the locations where there is IT equipment covered by this IT SAMP. There are three data center locations: Portland Headquarters, the Ross Complex, and Munro. Network equipment is located at each location marked by either a green or red dot on the map (the dot color is meaningful to Transmission's assets, but has no bearing on the IT equipment).

3.4 Demand Forecast for Services

Demand for IT products and services is expected to remain high over the next several years, and likely increase. Since IT is a business enabler, nearly every effort in the agency to support BPA's strategic goals depend on IT products and services. These generally take the form of new automation to support business processes, enhancements to existing automation, or the introduction of new technology to meet evolving business needs or compliance requirements.

Balanced against high demand for services is the underlying asset management objective that IT products and services deliver more business value than the cost of maintaining them at an acceptable level of reliability, availability, and

serviceability. This principle means that before we commit to implementing a new IT asset, we must also commit the future resources to maintain it. It means that we must engage in regular review of the business value and maintain strategic plans for retiring or replacing technology that is no longer cost-effective. IT must reserve the funding and prioritize the maintenance of IT asset life cycle activities such as preventive maintenance, repair and return-to-service, security updates/patches, vendor version upgrades to remain in support, end-of-life replacement, capacity management, continuous operations and disaster recovery capabilities, and performance monitoring. Funding levels, both capital and expense, must include the cost of maintaining current products and services, the cost of adding new products and services, and the ongoing operations and maintenance costs, including the rising costs of products and services and maintenance.

There are various factors that will continue to drive demand for IT products and services at BPA, some of which are as follows:

- Emerging Market Opportunities, such as WRAP – While BPA is in the early stages of defining what this effort may entail, IT can anticipate that it will require completing enhancements, replacements, or additions of several IT systems. From what we know so far, existing staff resources in CBS may be able to meet these required changes to existing applications.

- Compliance Initiatives – These can materialize at any time from sources such as Binding Operational Directives, Presidential or DOE Orders, federal legislation, NERC/CIP directives, etc. BPA is generally obligated to respond to these and in most cases to take direct action to meet the requirements.

- Shifting demographics – As newer generations of employees join BPA they expect more modern capabilities and personal use devices that support collaboration, social media, and mobility. These remain important as BPA continues to support a much larger telework and remote work presence.

- Cybersecurity threats – The proliferation of Cyber-attacks through multiple vectors will continue to drive faster adoption of security fixes in spite of the conservatism typically characteristic of the utility industry. Not only will this affect Enterprise IT systems, but also operational technology areas now exposed through the Internet of Things (IOT), and even reaching into the supply chain. One aspect of this that affects the cost of operating information technology functions is the rise in governmental mandates to implement specific cyber security architectures and practices, and to respond to ever-increasing data calls.

- Shift to the Cloud – While the rate of cloud adoption has slowed somewhat from the initial hype cycle, software vendors are increasingly moving to “cloud-only” options and charge higher premiums for traditional on-premise implementations. IT needs a secure and mature cloud strategy and cloud management capability. The transition has been lengthy and will require environments both on and off premise, which will drive changes in integration and infrastructure capabilities as well as approaches to asset selection. Typically characterized as expense-only projects, these are now a mix of expense and capital funding as Federal approaches have changed over time.

- Modernization of existing enterprise systems, such as Corporate Modernization – On the heals of Grid Modernization, BPA is considering the scope of a “Corporate Modernization” initiative that would seek to modernize the finance and other enterprise systems.

- Enterprise Asset Management Maturity (EAMM) program – In November 2021, the Enterprise Architecture Governance Committee (EAGC) approved a mulit-year collaboration between agency Asset Management, the Business Transformation Office (BTO), and Information technology (IT), in conjunction with business line asset management, to mature asset management capabilities across BPA. The program objectives are to plan for

enterprise asset management maturity, integrate business and maturity initiatives, steadily reduce technical debt, and ensure all teams working on projects related to asset management maturity remain aligned, supported, and informed. This workload has been adopted as an agency strategic outcome specific to Transmission's data systems, and is expected to work towards consolidation of asset management automated systems where practicable within Transmission to have an effective, reliable and repeatable process backed by efficient and right-sized technology solutions. This work has the long term potential to reach to other asset categories within BPA.

- Business Resilience – Traditional data backup and disaster recovery no longer adequately meet requirements for services to remain functional even during widespread disasters. Resiliency is the new descriptor, and is driving a faster approach to continuous operations that includes geographical failover for more than just critical business systems, and purpose-built data centers that consolidate resources.

3.5 Strategy Duration

The IT SAMP covers a five-year window and IT management reviews it annually. It is updated and published at least every two years. Due to the BPA power contract cycles, this version of the SAMP covers a 3-year period, FY2026-FY2028. Given the current velocity of change in asset management maturity, holistic strategy development and leadership fluctuation, IT anticipates a mid-cycle update of the SAMP. Drivers that may cause changes to the SAMP include:

- Rapid pace of change in IT hardware and software:
  - 3 years is a hardware life cycle, although a few outliers reach up to 7 years
  - 3-4 years is a software life cycle, although there are a few exceptions that are longer
  - Rapid adoption by industry of new disruptive technology (e.g., artificial intelligence)
- Evolving cyber security threats that require immediate counter measures
- New and disruptive federal regulatory requirements and directive orders (e.g., Cloud Smart, DOE Order 200.1.a, DCOI, CDM, ZTA, FICAM, IPv6, etc.)
- Changes to BPA business strategies and roadmaps – new business opportunities requiring new technology.

4.0 STAKEHOLDERS

4.1 Asset Owner and Operators

The Chief Information Officer (CIO) is responsible for overseeing the budgeting and procurement for all IT assets and services[1]. This includes initial implementation costs as well as on-going annual operational maintenance costs consistent with life cycle costing and the expansion of IT's sustain program to support any additional products and services.

[1] Under Federal Information Technology Acquisition Reform Act and BPA Policy 473-1, business units may budget and contract for IT services as long as the CIO maintains oversight of such actions and approves the procurement. However, executive management at BPA has a strong commitment to keeping the funding within the IT budget allocation, and exceptions to this are to be rare. The CIO

All assets and services are put in place in order to meet the business needs of the Information Owners[2] (IOs). The assets are maintained and operated by System Owners (SOs). SOs are IT managers or their delegates. SOs work with the IOs to ensure IT assets, services and automated systems:

- Deliver more business value than the cost to operate.
- Are maintained to reliably and securely meet current business needs.
- Satisfy industry and federal regulatory compliance requirements.
- Are enhanced to meet evolving and emerging business needs.

The IT Asset Plan, Facilities Asset Plan, and Physical Security Asset Plan have areas of mutual dependencies. Facilities provides key assets and resources needed to house and operate IT's networks and data centers. Physical Security provides access control and monitoring of key IT locations.

4.2 Stakeholders and Expectations

Table 4.2-1 describes the relationship between IT and its stakeholders. One of the most difficult to describe is the relationship between IT and the consumers of personal computing services. Stakeholder expectations for availability and support of personal computing services does not always align with IT's asset management plan. IT will work with consumers on an agreed understanding of expectations as it develops a more robust asset management strategy. This may help to curb the upward pressure on IT budgets to support a widening pool of services, devices, and software, and the commensurate staff and maintenance contracts to keep them operating at acceptable reliability levels.

Table 4.2-1, Stakeholders

Stakeholders	Expectations	Current Data Sources	Measures
Authorizing Official/ Chief Administrative Officer	Assets are maintained in a secure, reliable and operational condition, adhering to security controls documented in a General Support System (GSS) plan	General Support System plans	Audits
	Systems have a valid System Security Plan (SSP) and Authority to Operate (ATO)	System Security Plan (SSP) / Authority To Operate (ATO)	Audits
	Operating risks identified and mitigated to acceptable levels	SSP/ATO	Audits

and Supply Chain work in concert to identify and re-direct to the CIO any procurement actions initiated by a business unit for IT assets or services, but not approved by the CIO.

[2] The Information Owner is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, process, dissemination, and disposal. An Information Owner is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with other organizations. IOs are business unit managers (i.e., managers in Power, Transmission, Corporate, EF&W, etc.).

Stakeholders	Expectations	Current Data Sources	Measures
	Assets meet reliability objectives by being refreshed based on published refresh rates, and design meets availability requirments	IT asset inventories, AIM/ETS, IT Roadmap	Asset Health Indicators
Chief Information Security Officer	IOs/SOs have identified risks associated with IT Services mitigated to acceptable levels or excepted	SSP, ATO, SAR (Security Assessment Review)	Audits
	Timely resolutions of Program of Actions and Milestones(POAM)	POAM log	Audits
	Documentation of FISMA controls	Cyber Security Program Plan (CSPP), GSS, SSP	Audits
	Adherence to FISMA controls	IG, EA-21 Reports, SAR	Audits
Executive Board/ Administrator	Assets are delivering business value or are required to meet federal or industry regulatory compliance requirements	Information Owners	NEBR calculations
	Assets meet reliability objectives by being refreshed based on published refresh rates, and design meets availability requirments	IT asset inventories, AIM/ETS, IT Roadmap	Asset Health Indicators
	Capital investments are prioritized to achieve strategic objects, achieve/maintain compliance, and deliver business value	Project Management Office/PPM	PMO Work Plan
	Capital investments deliver cost effective solutions in a timely manner	Project Management Office / PPM	Project Investment Review
Information Owners	Systems are reliable and security maintained and meet availability requirements/SLA targets	Systems' Service Level Agreements (SLA)	Asset Health Indicators SLA targets/metrics
	Assets are enhanced to meet evolving and emerging business needs	Asset Plan, IT Roadmap	Asset Health Indicators
	New systems/automated solutions are delivered to meet evolving and emerging business needs	PMO Work Plan PMO Monthly Status Report	Project Health Indicators
IT Services Consumers (personal computing devices end users, etc.)	Modern, reliable desktop and mobile personal computing devices and system access	Customer Relations Management (CRM)/Technical Resource Request (TRR)	User satisfaction survey
	Modern reliable mobile communication services	CRM/TTR	User satisfaction survey
	Rapid delivery of software and peripherals	CRM/TRR	User satisfaction survey
Department of Energy/OMB/DHS	Compliance with DOE/OMB/DHS orders. Examples include orders to implement FISMA, DOE 200.1A, HSPD-12, IPv6, DCOI, FITARA, CDM, ZTA, etc.	Submissions to CPIC	Various data calls

Stakeholders	Expectations	Current Data Sources	Measures
	Timely resolution of POAM finding for DOE audits and security testing or risks are identified, documented, managed and mitigated to acceptable levels.	IG and EA 21 audits/reports	Resolutions of findings and POAM items
	DCOI: Reduction of data centers and PUE targets.	Submissions to CPIC	Number of tiered BPA datacenters (consolidation of DCC and HQ to VCC). PUE ratings of BPA tiered data center.
	Adoption of cloud-based services (OMB Cloud guidance).	Project Management Office Analysis of Solutions Alternative (ASA)	Each project ASA includes an evaluation of cloud-based services as a viable alternative.
General Public and External Customers	Access to BPA information to include news, environment information and activities, job opportunities, billing information, and metering information	Public facing web site(s) bpa.gov, Agency Enterpirse Portal, Pisces, Rate Recovery	User satisfaction survey

5.0 EXTERNAL AND INTERNAL INFLUENCES

IT experiences several external and internal influences as evidenced in table 5.0-1. Compliance considerations such as OMB directives and FITARA remain compelling. BPA cost consciousness and the rising cost of IT products and services have led to difficult choices in meeting both customer demand and compliance obligations. The IT SAMP describes these influences.

Table 5.0-1, External and Internal Influences

External Influences	Affects and Actions
OMB Cloud Smart Guidance Bonneville Power Administration is a federal entity with OMB direction to consider cloud-based solutions where they make sense from a cost and security perspective, which includes systems available through FedRAMP.	**Leveraging FedRAMP**, particularly for Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS), provides Bonneville with third-party evidence that a vendor meets FISMA moderate security control requirements. Our approach to OMB Cloud Smart **Guidance is to adopt cloud solutions** when the solution yields cost neutral to lower total cost of ownership. We have identified some use cases where cloud solutions meet these conditions; these include disaster recovery, development areas, and data analytics. We expect other use cases as cloud solutions mature. In this vein, we are encountering a number of situations where the vendor only offers Software-as-a-Service (SaaS). We currently have several SaaS solutions. Based on this guidance, we include cloud-based solutions as an alternative for all analysis of IT investments (projects).
Compliance Initiatives These can materialize at any time from sources such as Binding Operational Directives, Presidential or DOE Orders, federal legislation, NERC/CIP directives, etc.	The impact on BPA is to meet requirements outlined in compliance directives to which BPA must adhere. **The DOE Inspector General will challenge BPA to effectively address any shortcomings identified in DOE IG audits, related to compliance issues**. BPA will need to adjust priorities and budgets to allocate appropriate resources to accomplish the objectives and requirements of various compliance initiatives that may materialize at any time.
OMB Data Center Optimization Initiative (DCOI)/OMB M-16-19 and M-19-19 DCOI intent is to reduce the number of federal data centers and to require tiered data centers to achieve power efficiency targets.	The impact on BPA is to consider cloud-based solutions where feasible; achieve PUE targets via facility upgrades as necessary; and seek OMB permission to expand an existing data center or to establish a new data center. **OMB will challenge BPA to either use existing federal data centers or a cloud-based solution prior to expanding an existing data center**. BPA will need to adjust to operating in a hybrid mode where some services are on premise and others are off premise. In the meantime, planning for the replacement of the Dittmer Control Center with a new facility (VCC) offers the opportunity to **consolidate from three data centers to two** by providing space in the new facility to accommodate the HQ data center.
Federal Information Technology Acquisition Reform Act (FITARA)/DOE Order 200.1A (This may not be an "external influence" that has any major affects but does require an action – procurement of IT assets.).	**FITARA requires all IT acquisition to be overseen by the CIO**. As IT acquisitions that have been occurring in other organizations (often referred to as shadow IT) are identified and placed under oversight of the CIO, the IT budget and/or workload will increase. BPA Policy 473-1 requires procurement of all devices with an operating system or that are network addressable, and automated systems/servers, must occur under the oversight and approval of the CIO.
Trusted Internet Connection and IPv6 OMB directive is for federal entities to adopt trusted internet connections for inter/intranet connectivity and to transition from IPv4 to IPv6.	In 2008, OMB issued guidance to ready network backbones for IPv6. New direction is to now **convert all IP-addressed assets to IPv6** within a couple of years, approximately FY26. This has the potential to wreck havoc, especially for legacy software systems.
Rate of Change in IT An industry average server/laptop generation is about 2-2.5 years. Software is typically longer, about 3.5-4 years, with the possibility of extended support.	These short generations and rapid **obsolescence require a planned and sustained replacement program to maintain hardware reliability and to maintain software security and business value**. BPA has established refresh rates for all hardware components and recommends upgrades or replacement for software; however, BPA struggles to adhere to these established refresh rates as emerging business needs,

	and in some cases emerging security threats/vulnerability, often compete and are prioritized above mundane refresh plans/objectives.
Consumerization of IT (managing smart phones, tablets, and other consumer products) A combination of new personal devices (e.g., watches, fit bits, echo, Dropbox, social media, etc.) and the addition of operating systems and network addresses to traditional non-IT devices (e.g., refrigerators, coffee pots, etc.) has created a new class of IT-based devices primarily intended for consumer/individual use. As consumers become accustomed to and leverage these devices in their personal lives, they develop the expectation to have these devices available in the workforce.	**Staff expectation to use similar technology at work as they use at home** creates a number of challenges for IT. The first is ensuring these devices are used in a secure manner; in many cases the risks associated with these devices/services cannot be mitigated to acceptable levels. These devices were intended for personal use and lack the means to manage them at an enterprise level. The diversity of these devices makes it very difficult to train the staff that fix these devices when they malfunction. **The introduction of these devices increased the cost of IT services**. One way to manage the complexity from these devices is to introduce a combination of role-based provisioning and business requirements to determine which devices/services are provided to staff based on jobs and the business value these devices provide. **IT needs to transition to ensuring investment/project approvals are contingent upon the availability of expense funds to maintain them**.
Commodity material availability and cost uncertainty Higher costs for traditional IT equipment and software, and longer delivery time for vendors to provide products.	The impact to BPA is a shift and lengthening of schedule to accomplish lifecycle replacement activities for office automation, data center, and network portfolios. This potentially affects the entire PMO portfolio of IT projects, and may shift funding to subsequent fiscal years. Earlier planning, design, and procurement will likely be required.
Internal Influences	**Affects and Actions**
Maintaining an IT Investment Program IT expense budgets are nearly 100% consumed by O&M labor and contracts, largely due to rising costs of products and services (economic inflation plus additional use of existing products and services plus new systems) and rising cost of labor. Coupled with flat expense budgets, this limits the amount of work that can be accomplished.	New systems result in, on average, net new O&M costs of 8.2% of the investment cost due primarily to new software maintenance contracts and new support labor costs. Procurement costs have consistently come in higher than forecast. This has created a backlog in enhancements to existing systems and new systems as IT struggles to meet budget caps (insufficient expense available to move a project from initiate to execute, the phase where capital can be used). **Maintaining existing systems consumes nearly the entire IT expense project budget**.
Evolving Business Unit Roadmaps IT's capital investment funding is sized to meet identified business needs and infrastructure refreshes. Business units are in the process of completing their long-term strategies (business and geospatial strategies).	**The Business Transformation Office (BTO) works to reconcile strategies**. Once this work is done, IT and the Agency Prioritization Steering Committee will be able to create long-term capital investment work plans. Until a long-term work plan is completed, IT may find that it has underestimated the capital and expense needed to meet emerging business needs and/or investments in automated systems/services. These business needs will be delayed and/or go unmet.
Budget Constraints Budget constraints may push out developing and/or implementing strategic roadmaps, and may reduce maintenance capabilities.	**Budget constraints may push out developing and/or implementing strategic roadmaps** resulting in the delay of projects, which will shift spending to the out years. Budget constraints have also endangered the ability to meet annual increases in maintenance contracts, and delayed planned software refreshes, resulting in aging software with lower reliability, resulting in failing to meet business needs and potentially increased security risks and reduced reliability. Under current constraints, **IT is limited to funding personnel and maintenance contracts, with little capacity for new automation demands**.
Disaster Recovery (DR) General business systems do not currently have a viable disaster recovery site.	Under DCOI, expansion of an existing BPA data center will need an exception from OMB. BPA does have the option to use an existing federal data center that offers hosting services or cloud-based services for disaster recovery without requiring an exception from OMB. **DR is a required part of new system designs**; however, until a decision is made where to host DR, it will be difficult to enforce requiring new systems include DR as part of the delivered solution – the exception being cloud-based solutions.
Agency Asset Management Maturing asset plans and aligning IT with business objectives through asset plans (identifying out-year new projects/investments; creating multi-year roadmaps for existing systems/services).	IT, in conjunction with supporting BPA's Asset Management effort, is re-working IT asset plans to include proposals for out-year investments to align with business strategic roadmaps, business driven enhancements, operational costs, and refresh programs. **As the IT asset plans are matured, they will be used to identify resource requirements to achieve business needs and reliably operate and evolve existing systems and services**.
IT Workforce BPA expects to see 25% of its IT federal workers retire in 3 years and 50% in 8 years. Availability of skilled IT	IT workers have a lower unemployment rate than the national rate. This translates into a very competitive market of attracting and retaining skilled IT workers, including both Federal and supplemental labor resources. The federal hiring process is too slow and bureaucratic (from the applicant's point of view), has lower than appealing

workers at a labor cost that fits within IT budgets is a major challenge.	compensation rates, and does not support 100% remote work. This makes hiring talent with top skills extremely difficult. IT is developing a workforce strategy and Staffing Plan to ensure the workers with the right skills are hired to maintain and evolve IT services, and to **shift the use of supplemental labor to appropriate types of workloads**.
Electronic data growth Resources required to store electronic data have sustained growth rates of 25-30% over the last several years.	Not only does **the raw equipment required to store the growing load of electronic data** need to keep pace, but this also affects the ability for timely backup and recovery, the ability for automatic failover in continuous operations scenarios, and indexing and identification for eDiscovery.

5.1 SWOT Analysis

Table 5.1-1 describes IT's strengths, weaknesses, opportunities, and threats from an asset management perspective. After years of providing technology, IT is fairly mature at delivering operations. However, increased pressure to reduce costs, higher rates of security attacks, and the rising rate of conducting IT business threatens to increase down-time incidents and time to recovery.

Table 5.1-1: SWOT

Favorable	***Unfavorable***
Strengths (Internal)	***Weaknesses (Internal)***
• Credible and responsive customer service • Healthy partnership with the business lines for day to day operations • Strong Line of Business leadership, Information Owners, and product Owners engagement to drive improvement • Deep business domain knowledge of IT staff • Technical acumen and strong skills in operations, running and responding on software/incident response, system change management • Solid change management system to enable asset maintenance • Effective 24x7 support structure • Simple Capital Procurement Program • Incorparation of lessons learned (GridMod) • Documented System Life Cycle • Mature procurement processes	• Lack of structure for authority and decision making • Weak Organizational Change Management (OCM) • Situational understanding with a holistic current state view: lack of inventory automation, CMDB, regular update and validate processes • Weak business planning (prioritization & development), customers choose wanted solutions instead of requirements-based analysis • Lack of consolidated business line request process • Lack of enterprise business architecture, specific tools define processes, rather than processes defining tools • Lack of clear roles and responsibilities across orgs for vendor management • Planning for impact of capital procurements on expense O&M budget • System ownership understanding and agreement across orgs • Weak long term planning for replacements and upgrades asset lifecycle, and throughput analysis • Connection of enterprise architecture to technical architecture and understanding of roles and responsibilities • Staffing that is very O&M heavy; new work plus technical debt challenges, too focused on solutions • Weak requirements development, rationalization, and prioritization

Opportunities (External)	*Threats (External)*
• Improvements in secure coding skills • Developing/building an IT inventory and automated data capture • Improved stewardship of BPA owned IT assets: fully leverage current capabilities, consolidate tools, fund O&M to appropriate levels (maintain N or N-1 • Consolidation of enterprise asset management systems • Adoption of ITIL framework includes a CMDB to link assets to services • Maturing of IT Service Catalogue • Build-out of monitoring and mitigation capabilities	• Business line understanding and accountability of IT related costs • Misunderstanding of breadth and complication of IT implementation • Lack of cloud policy and architecture • Substandard security information from vendors • Unfunded compliance mandates driven by Executive Orders, Presidential Directives, and Binding Operational directives • Availability of funding for asset life cycle management • Rising rates of hardware and software maintenance contracts • Rising rate of technology change shortening asset life expectancy • Increasing security threats • Scarcity and rising cost of IT labor • Single points of failure for key IT systems • Loss of institutional knowledge resulting from retirements and attrition • In-flight changes to work priorities

6.0 ASSET MANAGEMENT CAPABILITIES AND SYSTEM

Using the Institute of Asset Management (IAM) Asset Management Maturity Model shows that the current state of IT asset management capabilities and systems continues to mature over time and has retreated slightly with an average maturity level of 1.2, about 0.4 lower than the 2022 assessment. The program assessment is conducted by the IT Asset Manager, agency Asset Manager, the Chief Information Officer, and the primary IT Asset Category Managers (the IT Tier-2 managers). Decision making and Life Cycle Delivery remain the strongest subject areas for IT. Strategy & Planning has experienced a slight increase in maturity due to the work of the IT Strategic Business Partners with our business line customers. Asset Information and Organization & People remain essentially unchanged although at a lower than desired level.

6.1 Current Maturity level

Asset Management Capabilities and Systems average a maturity level of 1.2 across all subject areas, which indicates a maturity between Aware and Developing on the IAM scale. This assessment shows a slight decrease in maturity level from the previous 2022 assessment as IT better unstands the assessment process and definitions, and the organization is generally tough on itself. In summary, IT is fairly good at keeping assets operational. It is marginal at resource management. There are a number of factors: IT uptime has been a major goal and metric for many years, resulting in IT assets that show a high level of availability. Budgets are generally top-down, maintenance contract costs are controlled by limited vendor competition, IT system rationalization at the customer level is sparse, IT asset life cycles are short, and long-range planning for IT assets is difficult, all leading to a reactive environment in which costs continue to rise and funding to maintain existing resources or add new resources remains scarce.

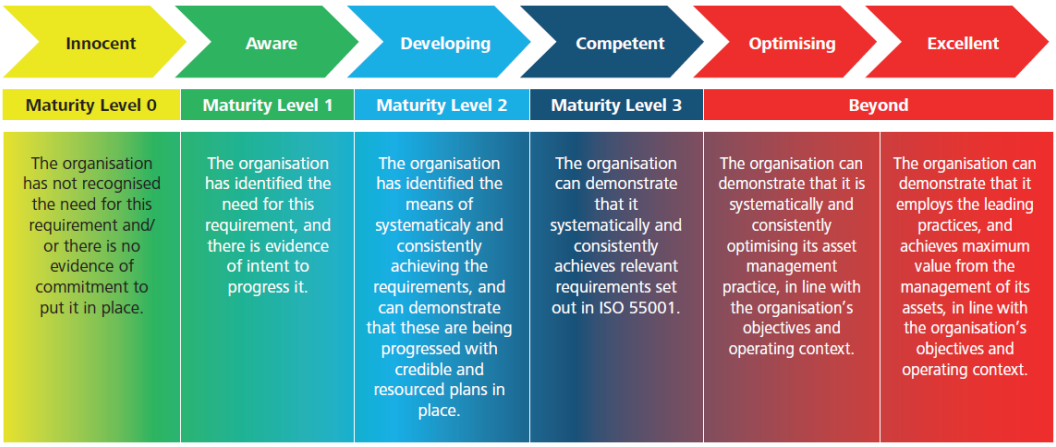
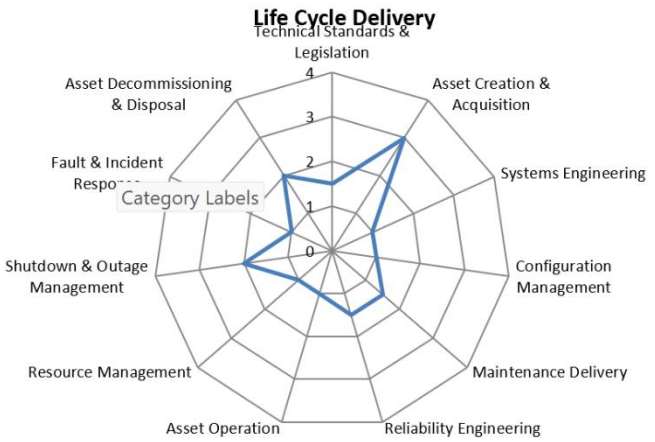
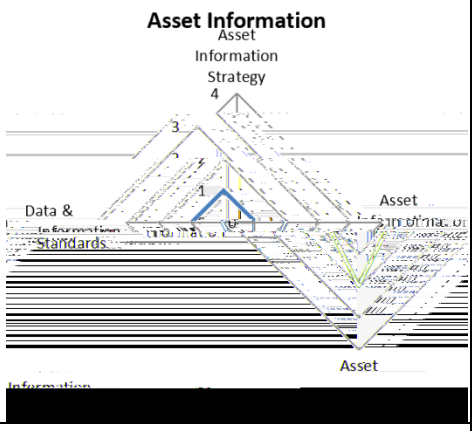
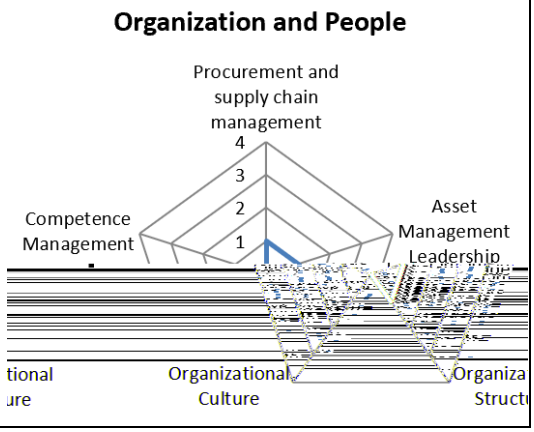


Table 6.1-1 identifies strengths and weaknesses within IT's asset management program and practices, based on the six subject groups of the Institute of Asset Management (IAM) framework and the IAM's maturity model.

Table 6.1-1 Maturity Level

Subject Area	Maturity Level
Strategy & Planning	Strategy and Planning within the IT organization is at a maturity level 1.4 (down from 1.6). **Strengths:** The IT organization understands the specific maintenance activities required to keep its assets in an operational condition. **Weaknesses**: Asset information has stagnated in some areas and are difficult to combine into coherent reports. Currency is at risk as we await an enterprise solution.
Decision Making	Decision-making within the IT organization is at a maturity level 1.6 (down from 2.2). **Strengths:** Capital investment decision-making is very mature. **Weaknesses:** Decisions to approve capital investments are not tied to/dependent on ensuring necessary expense required to maintain the assets in out years, and the IT expense budget is often cut to achieve BPA expense targets leaving IT with insufficient funds to maintain assets from investments.

Subject Area	Maturity Level
Life Cycle Delivery	Lifecycle Delivery within the IT organization is at a maturity level 1.5 (down from 2.1). **Strengths:** IT uses a documented System Life Cycle (SLC), which covers the acquisition of assets from proposal through production and eventual disposal. The SLC provides established baselines for consistency of business case, Analysis of Alternative Solutions, asset design, and defined standards for asset operation. **Weaknesses:** Maintenance and development team members are co-mingled, causing inefficiencies and suboptimal performance, and resulting in resource constraints to execute on approved projects. 
Asset Information	Asset Information in the IT organization is at a maturity level 1.3 (same level). **Strengths:** A Change Management Database (CMDB) is included with the enterprise IT service management tools that are currently under implementation. This could provide a common repository for all IT assets. **Weaknesses:** Asset information processes and governance around information are immature, and each sub-program stores its data independently. 
Organization & People	Organization & People in the IT organization is at a maturity level 0.6 (down from 1.0). **Strengths:** Procurement and supply chain processes are in place. **Weaknesses:** Organization and leadership strategy around asset management is lacking. Asset management is not a key factor in the IT culture. 

Subject Area	Maturity Level	
Risk & Review	Risk & Review in the IT organization is at a maturity level 1.1 (djown from 1.4). **Strengths:** Resources are available for peer review across portfolios and sub-programs. **Weaknesses:** The IT organization does not have well-defined processes or policies to identify, quantity and mitigate asset management risk ahead of End-of-Life emergencies.	

6.2 Long Term Objectives

The overall long term objective is to mature and assimilate sound asset management practices as defined by the Institute of Asset Management into IT's business processes. IT seeks to attain maturity level 2 (Developing) on the IAM scale in all six of the subject areas by the end of this SAMP period, FY2028. To meet this overall long term objective, we must focus on a few priority objectives related to Strategy & Planning, Life Cycle Delivery, and Risk & Review, defined below. Executing the related goals will improve those specific subject areas, and enable advancement in other subject areas as well.

- **Long Term Objective 1: Improve Strategy & Planning**
  - Educate IT managers on the Information Technology Infrastructure Library (ITIL) framework to transform the way in which IT provides, monitors, tracks, and evaluates service delivery to its customers. This will allow IT to measure its work capacity and consumption by customer demand to more effectively plan for service delivery and apply information technology assets to business operations, providing cost-value transparency.
- **Long Term Objective 2: Improve Life Cycle Delivery**
  - Work with IT customers and executive management to define and execute IT business processes that identify longer range adoption of IT automation solutions to business requirements through collaboration with business line customers. These processes must include executive support for prioritization in relation to agency strategic objectives and plans, culminating in application of existing or acquisition of new IT automation assets to facilitate business efficiency capabilities in support of business needs other executive initiatives.
  - Separate O&M staff from solutions development staff. IT has been saddled for years with the prospect of individual employees having to maintain operations of existing systems and also contribute to the development of augmented or new solutions to meet business line demand for IT products and services. When the same staff is assigned to both, each suffers, leading to unrealized maintenance activities and more and longer system outages, as well as delays in new system implementations which erodes their business value.

- **Long Term Objective 3: Improve Risk & Review**
    - Evaluating business resiliency requirements and using a risk-based approach, prioritize the build out of additional geographically dispersed or automated failover capabilities to improve resiliency of IT systems in support of business continuity objectives. This will improve BPA's ability to continue to operate and execute on its public mission in the face of impactful catastrophic events.

Table 6.2-1, Long Term Objectives

Subject Area	Goals	Timeframe	Sequence	Priority
Strategy & Planning	**Goal 1:** Measure work capacity and consumption to plan and execute service delivery.	Q4 FY27	1	1
Life Cycle Delivery	**Goal 1:** Define collaborative business processes to identify and plan for longer range automation solutions.	Q2 FY26	3	3
	Goal 2: Separate O&M support staff duties from development staff duties.	Q2 FY27	2	2
Risk & Review	**Goal 1:** Expand geographically dispersed or automated failover capabilities for high-impact business operations.	Q4 FY28	4	3

6.3 Current Strategies and Initiatives

Table 6.3-1 describes the current strategies and initiatives under way to support IT's long term asset management objectives, distributed over the IAM subject areas. These strategies and initiatives have either started or will start soon and will substantially complete on a shorter term, one to two years.

Table 6.3-1, Strategies and Initiatives

Subject Area	*Key Initiatives*
Strategy & Planning	**Initiative 1:** In November 2021, the Enterprise Architecture Governance Committee (EAGC) approved a mulit-year collaboration (Enterprise Asset Management Maturity) between agency Asset Management, the Business Transformation Office (BTO), and Information technology (IT), in conjunction with business line asset management, to mature asset management capabilities across BPA. The program objectives are to plan for enterprise asset management maturity, integrate business and maturity initiatives, steadily reduce technical debt, and ensure all teams working on projects related to asset management maturity remain aligned, supported, and informed. This initiative should produce a 5-year sequenced plan. **Initiative 2:** Shift major project prioritization to an IT/OT Governance Council focused on addressing technical debt and supporting a culture of innovation. Develop methods to obtain and document executive support. **Initiative 3:** Develop and publish IT Asset Management policies to strengthen what IT must do create a healthy AM function. **Initiative 4:** Develop charter and resource requirements to provide an IT Asset Management business function within IT. The charter should include support for business-line planning for specific technology needed to support the mission (define business value needed), definition of the minimum requirements for "business readiness" (requirements, process mapping, technology, and data) before investment requests are considered, and ensuring new technology investments have been evaluated from an enterprise perspective to maximize reuse of existing technology and ensure business requirements are clear before IT projects begin.

Decision Making	**Initiative 1:** Create business processes for joint business and IT planning for technology strategic needs to make improvements in planning for specific solutions and collaborative development of Strategic Asset Management Plans and Asset Plans, leading to integration with business goals and plans, and increasing the efficiency and effectiveness of IT projects. Major work efforts developed here will be considered by the new IT/OT Governance Council for prioritization.
Lifecycle Delivery	**Initiative 1:** The National Institute of Standards and Technology (NIST) defines the role of Information Owner (IO), which is a key contributor to asset management life cycles. While the role is assigned for IT automated systems at BPA, it is not well understood. To mature this capability IT will develop and deliver an IT-centric training course.
Asset Information	**Initiative 1:** Identify and document current state of assets and baseline IT capabilities. Define critical data points (and add new data points) required to determine IT asset criticality, health, and risk scores, including a deterministic mathematical method to assign scores. Develop sustainable processes and procedures to collect, store, and analyze this data for all IT assets.
Risk & Review	**Initiative 1:** Leverage the new health and risk score indicators to inform budget planning and prioritization of IT asset life cycle activities, and mitigate technical debt. **Initiative 2:** Balance cyber risk, compliance requirements, and business needs in all risk, reliability, and prioritization-related business processes. **Initiative 3:** Expand monitoring capabilities to identify and mitigate both operational and cybersecurity risks through implementation of the Network Security Operations Center (NSOC) and additional build-out of the existing Cyber Security Operations and Analysis Center (CSOAC).

6.4 Resource Requirements

To accomplish the IT long term objectives and current initiatives a combination of existing staffing resources, new staffing resources, and IT products and services will be needed, including ongoing O&M expenses such as annual software and hardware support costs. Most of these resources will likely be permanent staff, while some staff will be short-term temporary contracted resources. Additional staff resources will be required to provide oversight and reviews.

Detailed resource requirements will be included in the annual IT asset plan.

7.0 ASSET CRITICALITY

7.1 Criteria

IT does not currently have a deterministic mathematical model to determine criticality scores for specific IT assets. The short-term initiative number 1 for Asset Information in Section 6.3 descrbes at a high level IT's intent to create such a model. In the meantime, IT uses a logical flow to determine asset criticality:

Critical Business Systems (CBS) are mission critical in the sense that they provide or directly support revenue generation for the agency. These include systems such as trading floor applications, power scheduling, weather forecasting, power metering and billing, and all of the IT hardware and software components that support their operation (network cabling and routers and switches, firewalls, telephones, servers, electronic storage, desktop user interfaces, etc.)

Cyber security systems are mission essential in the sense that they provide monitoring and protections against cyber threats that could compromise data or operations for any interconnected IT systems.

Enterprise Business Systems (EBS) are very necessary in the sense that they provide basic automated administrative business functions in support of agency daily operations such as Human Capital Management, Fleet and Facilities inventory, and agency financials.

Best effort is all assets that don't fall into one of the first three categories.

Once an IT asset is identified to reside in one of the four categories describe above, additional criticality modifiers are considered:

The environment in which it resides (most to least critical): Production, Failover, Test, Development.
The operational area in which it resides (most to least critical): Reliability, Compliance, Policy Commit, Discretionary.
Financial impact to the agency of reduced performance or failure (currently subjective).

Table 7.1-1 Examples of IT System Criticality

Business Function	Systems	Classification & Ops Area	Contribution of Service	Impact of Failure/ Business Continuity
Real time or preschedule Scheduling	Integrated Scheduling Accounting and After the Fact Calculator (ISAAC)	CBS / Policy Commit	Integrated Scheduling Allocation ATF & Calculation.	BPA would be unable to manage schedules to loads and transmission constraints. Critical 24x7 20 min return to operations in place.
Hydro Operations	Hydro Regulation Model System (HERMES)	CBS / Policy Commit	Model for developing hydrologic forecasts for Power Services and other business operational requirements; keeps BPA in alignment with the NWS and other federal agencies.	BPA would be unable to model for FCRPS water condition, which would impact our ability to predict how much "fuel" is available in the system in the short, mid, and long term. Critical 24x7 20 min return to operations in place.
Marketing (deal capture, day ahead trading)	nMarket	CBS / Policy Commit	Enables bidding, dispatch and settlement processes between BPA and the CAISO. Real-time traders and CA Market staff will bid into the CAISO market using nMarket.	nMarket: BPA would not be able to bid, dispatch, or settle transactions in the CAISO. This would directly affect BPA's commercial operations. OATI: BPA would not be able to manage tags or Transmission service requests, Available Transmission capacity, transmission schedules and reservations, nor check out with adjacent BAs. Trade Management System: BPA would be unable to manage the bulk marketing revenue from surplus power sales. Critical 24x7 20 min return to operations in place.
	OATI	CBS / Policy Commit	Interface to the Energy Industry Registry (EIR) for registering & maintaining company information as required by the North American Energy Standards Board (NAESB). Allows TBL scheduling staff to process and manage E-Tags.	
	Trade Management System	CBS / Policy Commit	Provides a common IT platform to effectively manage the Agency's PBL Secondary Revenue. This system enables the functional areas of the Front, Middle, and Back Office.	

Business Function	Systems	Classification & Ops Area	Contribution of Service	Impact of Failure/ Business Continuity
Asset Management	Transmission Asset System Cascade	EBS / Discretionary	Provides a comprehensive equipment nameplate database to track and schedule routine inspections, tests, and servicing of transmission equipment. Supports asset health determination. Used in developing and modifying asset maintenance plans and supporting decisions to repair, replace or retire assets.	If unavailable Transmission's ability to maintain critical transmission equipment would be impacted and could potentially result in WECC violations due to NERC/CIP requirements for maintenance.
	Asset Suite	EBS / Discretionary	Work Management and Asset Management system. A component of BPA-wide Enterprise Resource Planning.	If unavailable for more than one week, the business would have to rely on manual processes to continue business operations. Some compromised processes could include: • Inability to record project and work order status for financial reporting, maintenance tracking. • Inability to procure and distribute supplies and materials for necessary maintenance and construction activities • Inability to process service contracts, power contracts and make payments to vendors, thus incurring interest penalties and potentially losing lines of credit or preferred status. • Unable to process and make supplemental labor (SLMO) payments.
	Telecommunications Circuit Information System	EBS / Discretionary	Manages telecommunication circuits including Framework, Resource Inventory, and Design & Planning.	BPA's Operations staff would be unable to determine the effects of circuit outages on the transmission system.
Financial Services	Billing Invoice System	EBS / Policy Commit	Manages Power and Transmission billing and backup documents, and associated customer attributes.	Decreased ability for BPA to document or defend bills sent to our customers over the last 10 years.

Business Function	Systems	Classification & Ops Area	Contribution of Service	Impact of Failure/ Business Continuity
	Financial Management System	EBS / Compliance	Enables Accounts Payable, Accounts Receivable, Projects, and GL.	In the event FMS becomes unavailable for an extended time, BPA's financial information and accounting processes would be severely impacted. Some of the compromised operations could include: • Inability to receive incoming revenue. • Inability to make vendor and contract payments, thus incurring interest penalties and potentially losing lines of credits or preferred status. • Unable to close month-end/year-end. • Unable to account for assets and/or liabilities. • The extended unavailability of the BPFAS system would result in the inability to develop budget data, which may put BPA in non-compliant status for external requirements, such as OMB circular A-11. In addition, this would negatively impact BPA's financial communication with the public and other government entities as well as our internal cost management efforts.

7.2 Usage of Criticality Model

The asset criticality and associated criteria are used for decision making in two primary instances: 1) Responding to live asset performance anomalies, and 2) Planning for asset life cycle activities. The former is a typical IT operational activity where the system criticality determines the level of effort of response personnel to return asset technical performance to acceptable levels. In some cases, this also includes maintenance activities undertaken to reduce risk of failure and extend asset performance.

The latter instance, major life cycle activities, uses the criticality and associated criteria to inform budget formulation early in the fiscal year, and again to prioritize projects related to adding new systems, updating systems, replacing systems, or retiring systems. The Agency Priority Steering Committee (APSC) is a cross-organizational body facilitated by IT that evaluates these project submittals and assigns relative priority based on the criticality criteria, and recommends actions to the Chief Information Officer for approval. There are additional business-related criteria used by the APSC to help determine priority levels, such as cost and business readiness. The APSC also tracks project performance and approves progress through the System Life Cycle (SLC) gateways. IT's charter, as well as the System Lifecycle (SLC) documentation is maintained by the IT Project Management Office.

The use of the criticality logical flow provides a good starting point for determining priority of activities when a conflict in resources arises. However, there are additional factors that also influence work prioritization decisions such as point-in-time considerations. An example of this is the year-end financial closing in late September and early October of each year, during which system changes are severely restricted. It is also important to understand that the criteria described is not

specificially programmatic, meaning that subjective discussion is required to come to a conclusion where the criteria may be contradictory under specific circumstances. There are combinations of criticality factors across the logical flow that may require this collaborative adjudication by the IT service manager and the client stakeholders. For instance, is a Compliance issue in the Test environment more or less important than a Discretionary issue in the Production environment? Business impact at that point in time would be a major consideration for that decision.

8.0 CURRENT STATE

IT assets are acquired to automate and support BPA business functions and to enable worker productivity. Key asset measures need to be aligned with enabling business units to achieve their objectives with a net positive value. Key IT measures include reliability, security and Business Reliliency.[3]

8.1 Historical Costs

Table 8.1-1 shows the historical spend based on project actuals and projections as reported through the IT Project Management Office. Note that while this table includes all capital expenditures in IT, the expense O&M expenditures only include those that supported the IT PMO projects, and the total IT expense budget is included in the last row.

Table 8.1-1 Historical Spend

Program	Historical Spend (in thousands) With Current Rate Case						
Capital Expand (CapEx)						Current Forecast or Rate Case	
	2019	2020	2021	2022	2023	2024	2025
Applications	$2,110	$8,700	$5,020	$2,624	$239	$99	$5,000
Data Center		$2,800	$480	$668			
Network							
Total Capital Expand	$2,110	$11,500	$5,500	$3,292	$239	$99	$5,000

[3] Business Resiliency component overlaps with both reliability and security. Security includes availability, which Business Resiliency addresses. Reliability includes recovering from services disruption, which Business Resiliency addresses for catastrophic failures.

Capital Sustain							
Applications	$2,190	$1,300	$9,718	$9,623	$5,888	$16,937	$7,337
Data Center	$1,748	$5,326	$7,000	$2,452	$3,352	$2,286	$3,150
Network	$3,700	$2,600	$2,600	$4,435	$6,225	$4,245	$5,850
Total Capital Sustain	$7,638	$9,226	$19,318	$16,510	$15,465	$23,468	$16,337
Expense (OpEx)							
Exp to execute IT PMO work	$11,530	$6,436	$6,740	$6,488	$5,793	$5,485	$1,774
Total Expense	$96,400	$95,800	$101,800	$109,100	$115,800	$121,000	$126,000

Figure 8.1-1 depicts the asset spending for the last five years. All capital spending is captured through the IT Project Management Office. All of IT's expense spending can arguably be described as related to IT asset management, so it is included here as a total sum and the expense required to execute IT projects is a subset of the total sum. IT does not track all expense spending by asset portfolio.

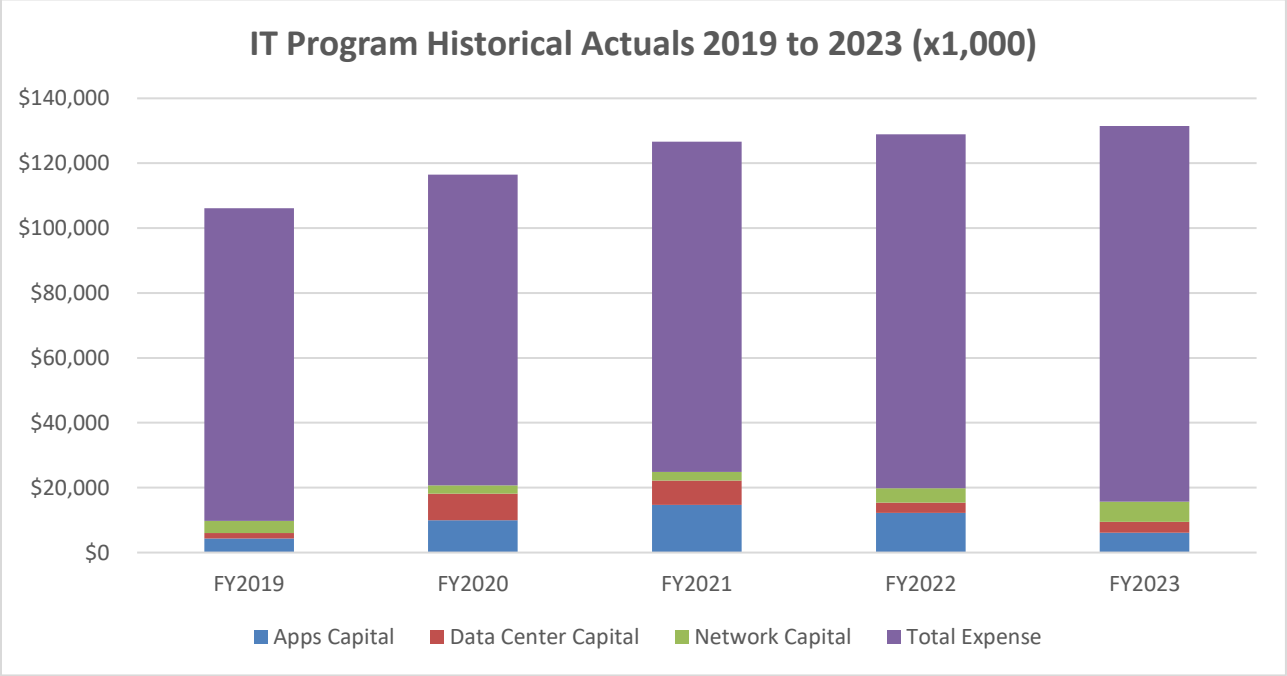


Figure 8.1-1 Historical IT Program Expenditures

Figures 8.1-2 and 8.1.3 show the asset expand and sustain spending for the last five years. All capital spending is captured through the IT Project Management Office, as well as the expense spending required to execute on those specific projects and expense-only IT PMO projects.

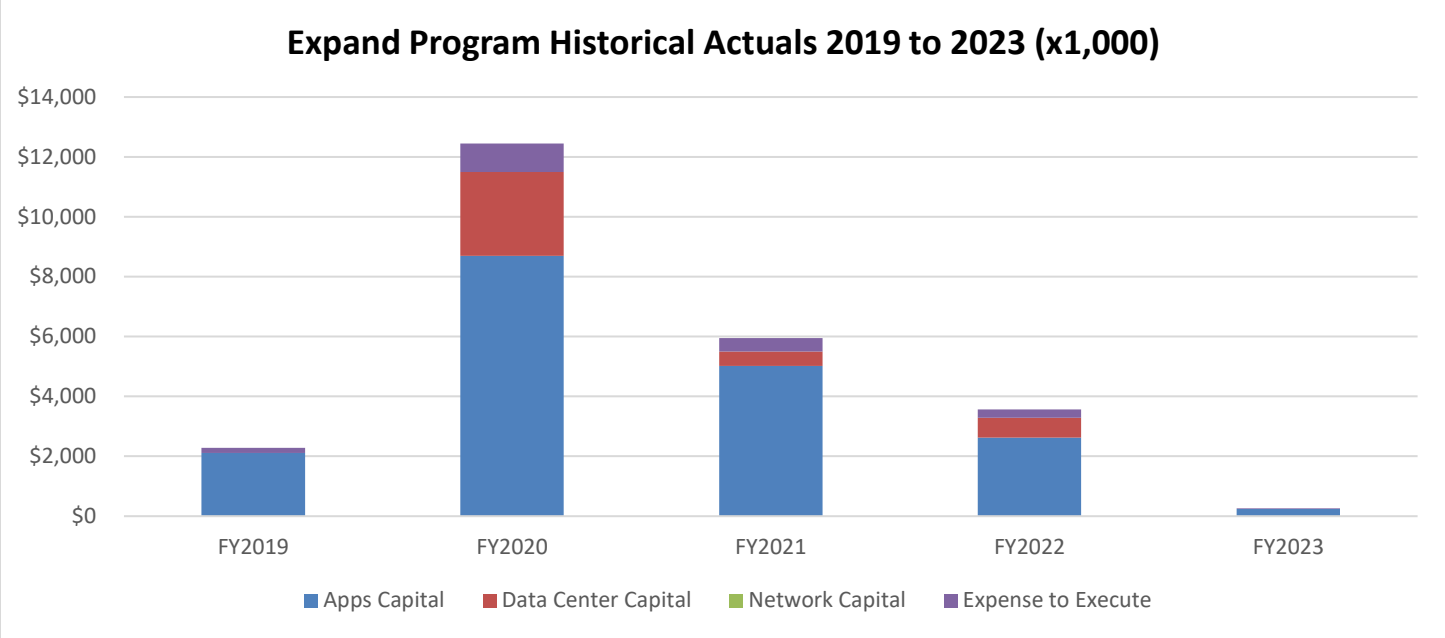


Figure 8.1-2 Historical Expand Program Expenditures

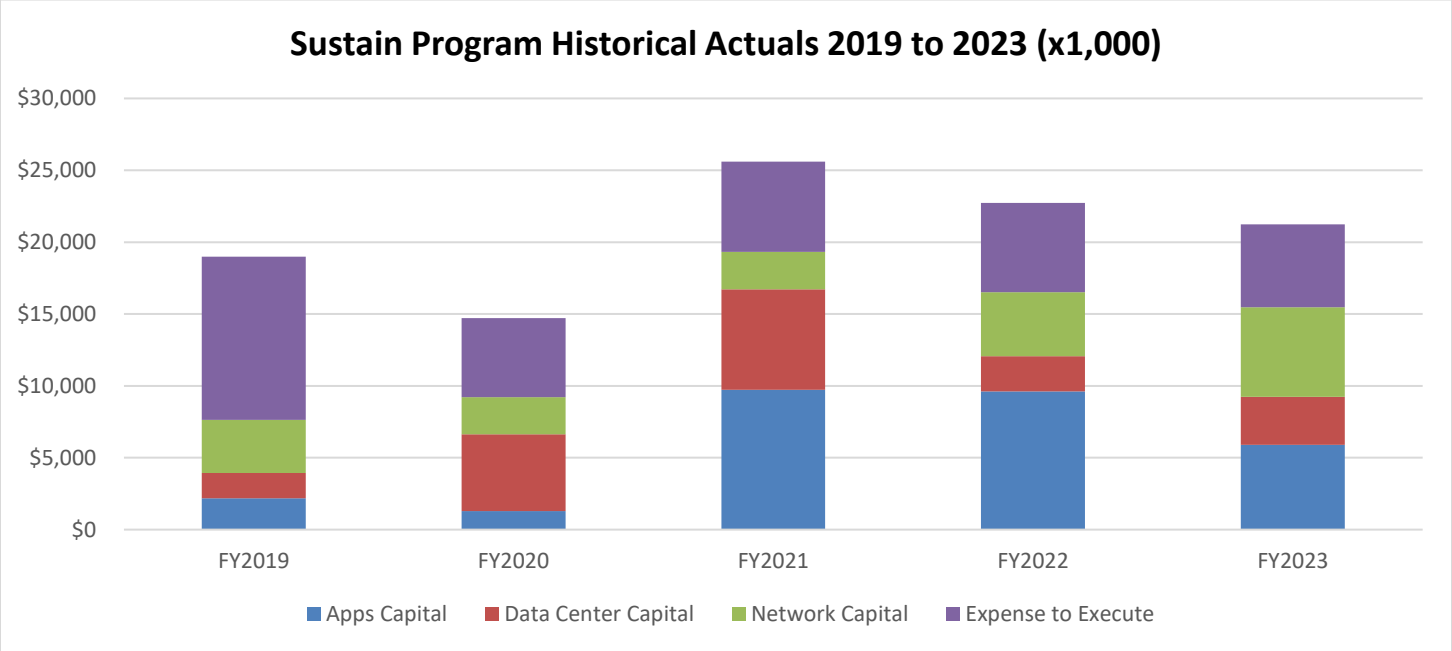


Figure 8.1-3 Historical Sustain Program Expenditures

As shown in figures 8.1-1 through 8.1-3 spending priorities within IT have shifted from expand activities to sustain activities in order to maintain reliability and availability of existing systems. This is expressed by the idea that if BPA invests in obtaining IT assets, those assets must be maintained. The maintenance includes both infrastructure and software. Infrastructure is made up of both the hardware and lower level software that enables application performance and user access, and the applications used to enable business performance. Failures in either area increase risk to cyber security and risk to meeting business objectives.

While this shift in prioritiy of spending has helped to address asset health in some areas, O&M funding levels remain inadequate in the face of rising cost of labor and asset maintenance contracts, and normal customer demand increases. The result has been limited resources to maintain service and asset health, increased single points of failure for IT functions, and stretching certain application life cycles beyond limits. Additionally, expense funding to consider new expand efforts to meet emerging business needs is essentially non-existant and will remain so through FY25.

Two factors have helped to mitigate the limited availability of expense funding in relation to asset health:

- Infrastructure assets for data center and network typically meet capitalization thresholds and require little expense funding to execute life cycle replacement activities that retain asset health. The annual Simple Capital Procurement program has been able to remain in alignment with asset goals.
- Shifting the Office Automation asset to leased rather than owned equipment has changed the funding profile from expense and contractually defined the life cycle replacement of Office Automation assets. These asset replacements can no longer be considered for deferral to meet budget targets.

However, these activities are not without their challenges such as limited staff resources, global supply chain delivery issues, and coordination with clients that work in maximum telework environments.

8.2 Historical Asset Sustain Trends vs Forecast

IT has generally only considered this type of information for specific projects that have been prioritized and approved, not for the whole portfolio of IT assets. However, the optimal goal for replacement execution is currently determinied by the established life cycle replacement period for each asset. While some specific assets may have differing periods, the average for infrastructure hardware is 3 years and for applications is 4-5 years. The infrastructure hardware is generally meeting the goal, whereas applications are trending to fall further behind and grow the existing backlog. This is largely due to limited expense funding that results in understaffing and curtails the ability to maintain effective rates of replacement.

This SAMP intends to outline and request FY26-FY28 actions and resources to improve the sustain execution rate as well as to provide capacity for customer demand expansion as much as possible. Potential programs include such things as:

- Stabilize Critical Business Systems
- Stabilize Application Support Services

- Converged Infrastructure services
- Desktop Delivery
- Server and System Operations

8.3 Asset Condition and Trends

Asset conditions and trends are predicated on an accurate inventory of assets and the conditions of those assets based on certain criteria. The approach to defining asset counts is also important. IT is in the process of refreshing inventory data at this time, so the data presented below is somewhat dated and will change as new information is collected. However, the infrastructure assets likely remain fairly constant, whereas the application assets have likely declined in condition to a small degree. Additionally, IT has identified improvements in the condition criteria and asset identifications that it plans to develop during the SAMP and AP cycles. Some examples of this include vendor End-of-Life and End-of-Support dates, separation of unit components where it makes sense, how we report out spare equipment, etc.

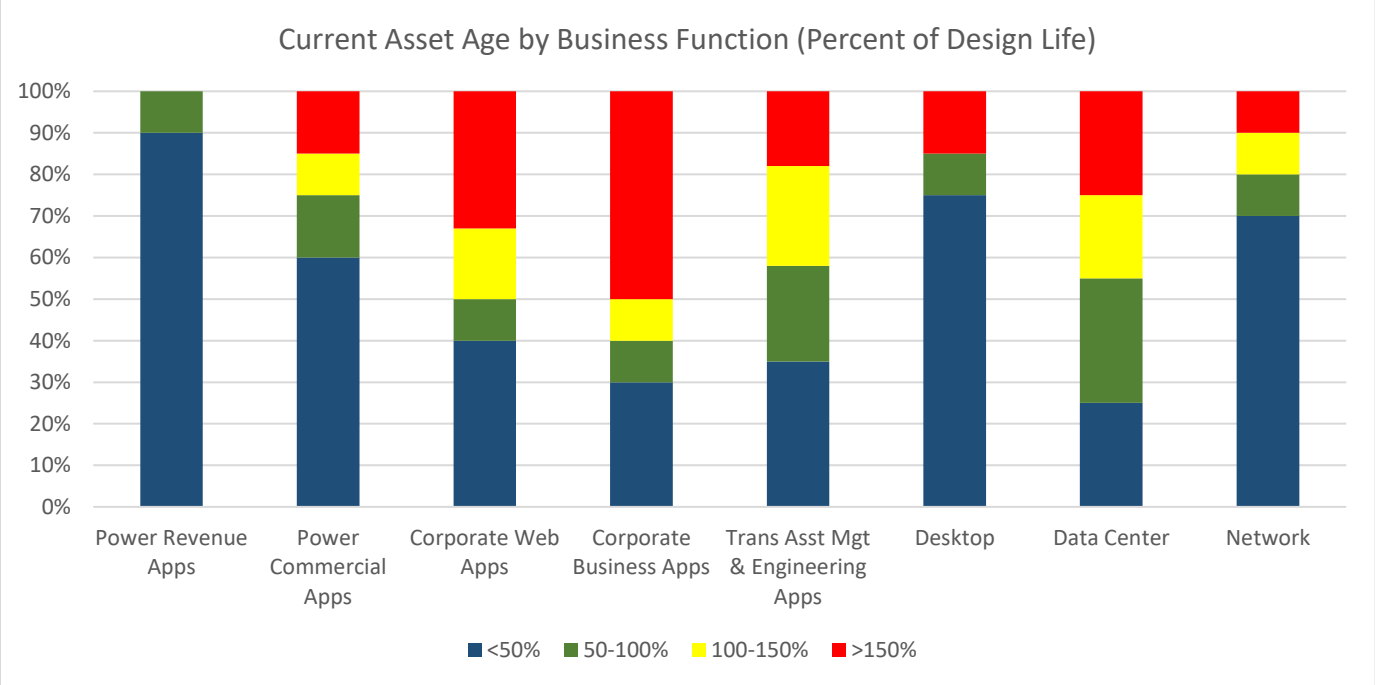


Figure 8.3-1 Current Asset Age by Business Function

Figure 8.3-1 reflects the condition of the software systems supporting business functions (Power Revenue Apps, Power Commercial Apps, Corporate Web Apps, Corporate Business Apps, Transmission Asset Management and Engineering Apps, and the underlying infrastructure that enable the apps to operate: Desktop, Data Center, and Network services). For Computer Off-the-Shelf (COTS) systems, the conditions are a reflection of vendor support and IT's currency with the vendor's most current mainstream supported versions. For in-house developed systems, the conditions reflect how well it is being updated (enhanced) to meet evolving/emerging business needs. It should be noted that for Software as a Service (SaaS), these cloud-based solutions undergo continuous updating by the vendor and should always be blue or green unless the vendor has announced phasing out support for a given solution.

With the number of applications in the IT portfolio, managing asset conditions to within N-1 versions and additional customer demands, with limited expense funding to maintain staffing levels, is a serious challenge. As IT refreshes its application inventories and updates condition criteria, combining that data into the IT Roadmap will highlight specific applications of primary criticality and concern. Overall, the two largest areas of concern are estimated to be Corporate Web Apps, which are currently undergoing upgrades to return them to acceptable levels, and Corporate Business Apps, which are being evaluated for a major upcoming overhaul (Corp Mod) that could include most of our Enterprise Resource Planning tools (i.e. Human Resources systems).

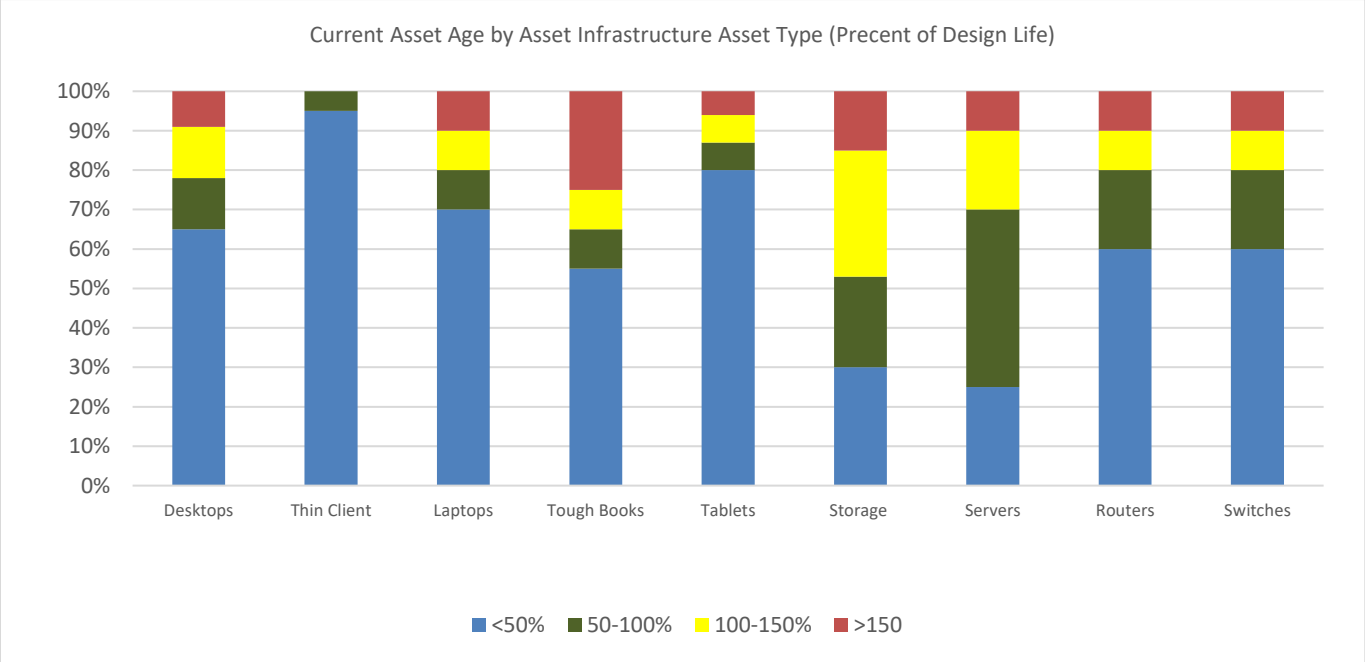


Figure 8.3-2 Current Asset Age by Asset Type

Figure 8.3-2 concentrates on the physical assets described within Infrastructure assets: Desktop equipment, Data Center equipment, and Network equipment. It shows the relative age distribution for the various types of equipment.

Desktop equipment is in much better shape now than in the last several years due to wholesale upgrades based on equipment leases. Network equipment has been on an annual percentage upgrade path for some years, and the pattern there is expected. Servers and storage have changed from a more forklift (complete upgrade over a short period) strategy to an annual percentage refresh. This will shift the assets more into the blue assessment, particularly as we prepare to migrate data centers from HQ to the new Vancouver Control Center facility in about FY2029.

Of most concern is the operating system versions on the servers. Dependencies between the host operating systems and the applications that run on the host can be complicated and require additional staff time for addressing obstacles, user testing, etc. Limited staff resources have caused delays in this area, creating a backlog of deferred updates and increasing vendor maintenance costs and cyber security risks.

8.4 Asset Performance

IT has generally adhered to traditional industry measures such as functional uptime statistics for servers and networks, while measuring reliability of desktop systems via Service Desk metrics such as number of tickets serviced in various categories of support. And while service level agreements have been in place for some time between IT system owners and client stakeholders, not all systems have them established.

IT has been slow to fully develop, mature, and track a set of robust measures that captures asset condition and gauges progress in achieving objectives. IT developed a set of five metrics to measure the health of IT assets, however reductions in staffing have prevented their adoption. The intended metrics are as follows:

- Reliability - Measures the asset's ability to deliver capabilities without disruption of service or operations. Metric is intended for hardware and for software systems.
- Financial Value - Intended to be applied to discretionary systems where the annual cost of operations may be greater than the annual business value being provided by the system.
- Business Needs - Measures how well the solution is meeting business needs. Requests for high levels of enhancements indicate the solution is not meeting current or evolving business needs. This is an indication that either a major upgrade is needed or a new solution may be needed to meet current and/or future business needs.
- Security and Risks - Measures if the asset is adequately addressing security (POAM items) and risks.
- Business Resiliency - Measures the asset's ability to meet Business Resiliency requirements.

Additional considerations are:

- Safety – No direct impact from IT assets other than stretch relationships such as public safety issues if the power grid fails due to a computer system outage.
- Environmental – IT uses Energy Star components so no additional measures are necessary.
- Compliance – Affects prioritization of IT projects and therefore schedule and budget. This will be considered for future addition.
- Natural Resources – No direct correlation to IT asset performance other than supply chain availability, for example delivery time of assets may be affected by global supply of silicon affecting chip production.

Table 8.3-1 describes the intended goals for each of the above metrics with green indicating acceptable, yellow marginal, and red needing mitigation.

Table 8.3-1 Intended IT Asset Health Indicators

Metric Name/Measure	Green	Yellow		Red	
	Condition	Condition	Remedy/Action	Condition	Remedy/Action
Reliability: Measures the asset's ability to deliver capabilities without disruption of service or operations. Metric is intended for hardware and software systems.	Asset is meeting stated availability objective (if no availability objective is stated, the assumed objective is 98.5% availability).	Asset availability objective is not defined and/or is not being tracked.	ISO works with IO to define availability. ISO either begins tracking availability or creates activity in Asset Plan to enable tracking.	Availability objective is not being met.	ISO creates activity in Asset Plan (upgrade, bug fix, enhancement, or replacement) to achieve availability objective. Executes upon availability of resources.
	For hardware, the asset is more than 2 years from its scheduled refresh rate and the asset plan contains an activity to refresh the asset.	If hardware asset is within 2 years of its scheduled refresh, upgrade, or retirement and there is an activity in the asset plan to execute one these actions.	Ensures activity in Asset Plan to replace hardware on scheduled refresh date. Performs refresh on or before refresh date and ensures an activity is in Asset Plan for next refresh.	Hardware is beyond scheduled refresh date.	Refresh hardware. Ensure activity is in Asset Plan for next refresh cycle.
	For software, the software has more than 2 years before its next major upgrade or retirement date and the asset plan contains an activity to upgrade or retire the asset.	The solution (including components) is one version back (N-1) of current major version.	Ensure activity is in Asset Plan for upgrade. Perform upgrade on schedule. Ensure activity is in Asset Plan for next upgrade.	Solution (including components) is at more than one version (greater than N-1) of current major version.	Perform upgrade on schedule. Ensure activity is in Asset Plan for next upgrade.
		The solution (including any component) is more than one year and less than two years from vendor's end mainstream support.	Ensure activity is in Asset Plan for upgrade/replace. Perform upgrade/replace on schedule. Ensure activity is in Asset Plan for next upgrade/replace.	Current version prevents security patches from being applied to the operating system.	Perform upgrade/replace on schedule. Ensure activity is in Asset Plan for next upgrade/replace.
		The solution is more than one year and less than two years from vendor's end of life for the product.	Ensure activity is in Asset Plan for replacement. Perform replacement on schedule. Ensure activity is in Asset Plan for next upgrade.	Current version prevents the operating system from being upgraded to at least one version back (N-1) of the current major version of the operating system.	Perform upgrade/replace on schedule. Ensure activity is in Asset Plan for next upgrade/replace.

Metric Name/Measure	Green	Yellow		Red	
	Condition	Condition	Remedy/Action	Condition	Remedy/Action
				Solution (includes any component) is less than one year from vendor's end of mainstream support or end of life.	Perform replacement on schedule. Ensure activity is in Asset Plan for next upgrade.
Financial Value: Intended to identify discretionary systems where the annual cost of operations is greater than the annual business value provided by the system. Remedy/Action is intended for discretionary systems with annual operation costs of more than $150K per year.	The Net Economic Benefit Ratio is being tracked and updated annually.	The annual benefits are not being tracked.	The information Owner ensures the business benefits are defined and are being tracked.	Red when the annual operating costs are greater than the annual benefits.	An activity (enhancement or project) must be placed in the asset plan to increase annual benefits above annual operating cost.
	The annual benefits are greater than the annual operating costs.	The annual benefits are not defined (should this be a red criteria?).			A proposal must be placed in the asset plan to replace the system.
	Identified annual benefits are less than $150K/year.	The annual operating costs are unknown.	The information System Owner ensures costs are being tracked.		Retire the system.
		If the system "Financial" asset condition has not moved yellow to green after 2 years, the system must be retired at the end of the third year unless: • A enhancement or project is flight to drive the annual benefits to be greater than annual cost of operation. • The Information Owner has requested and received an exception from the IT Asset Manager.		If the system "Financial" asset condition has not moved red to green after 2 years, the system must be retired at the end of the third year unless: • An enhancement or project is flight to drive the annual benefits to be greater than annual cost of operations. • The Information Owner has requested and received an exception from the IT Asset Manager.	
Business Needs: Measures how well the solution is still meeting business needs. High levels of enhancements indicate the solution is not meeting current or evolving business needs.	Annual enhancement cost is less than 25% of operations and maintenance costs.	Annual enhancement costs exceed 25% of operations and maintenance costs for 2 or more consecutive years.	ISO works with IO to determine if system needs to be upgraded, replaced, or other action is needed to reduce enhancement costs. Update Asset Plans with activities to control enhancements.	Annual enhancement costs exceed 50% of operations and maintenance cost for 2 or more consecutive years.	ISO works with IO to determine if system needs to be upgraded, replaced, or other action is needed to reduce enhancement costs. Update Asset Plans with activities to control enhancements. ISO works with IO to
	The enhancement costs in any given year exceed 20% of the initial investment.	If enhancement costs in any given year exceed 20% of the initial investment.		Enhancement costs in any given year exceed 20% of the initial investment.	

Metric Name/Measure	Green	Yellow		Red	
	Condition	Condition	Remedy/Action	Condition	Remedy/Action
This is an indication that either a major upgrade is needed or a new solution may be needed to meet current and/or future business needs.	The estimated backlog of enhancements is greater than $75K.	The estimated backlog of enhancements is greater than $75K.	ISO works with IO to ensure enhancements are needed and provide more business value than the cost of the enhancements.	The backlog of identified enhancements exceeds an estimated $150K to complete.	ensure enhancements are needed and provide more new business value than the cost of the enhancements.
	The cumulative cost of enhancements is less than 10% of investment.	The cumulative cost of enhancements is greater than 20% of investment.	ISO works with IO to determine trajectory of enhancements; if increasing, determine if system will need future upgrade or replacement.	The cumulative cost of enhancements is greater than 50% of investment.	
				The cost of enhancements exceeds the business benefits from the enhancements.	
Security and Risks: Addresses if the asset is adequately addressing security (POAM items) and risks.	No Active/open POAM items.	Asset Plan contains activities to close all open POAM items.	Execute on activities in Asset Plan and close POAM items.	No activities in Asset Plan to close POAM items and/or items have been open for more than 12 months.	Enter activities into Asset Plan. Execute on activities to close POAM items.
	No risks with probability higher than "Possible" and impact higher than "Moderate."	Asset plan contains activities to mitigate risks identified in IT Asset Strategy or other IT risk registries to acceptable levels (either probability below “Possible” and/or Impact is mitigated below “Moderate”).	Execute on activities in Asset Plan to mitigate risks to acceptable levels.	No activities to mitigate identified risks (probability above “Possible” and impact greater than “Moderate”) to acceptable levels and/or risks are older than 24 months.	Enter activities into Asset Plan. Execute on activities to mitigate risks to acceptable levels.

Metric Name/Measure	Green	Yellow		Red	
	Condition	Condition	Remedy/Action	Condition	Remedy/Action
	The system has a geographically separate failover location, which is outside of the Cascadia subduction zone and system can failover, meeting both RTO and RPO.	There is activity in the Asset Plan to establish geographical failover capabilities that meets RTO and RPO.	Establish geographical failover that meets RTO and RPO.	If there is no activity in the Asset Plan to establish geographical failover capabilities.	ISO works with IO to define RTO and RPO. Ensure activity is in Asset Plan to establish failover. Execute on activity to establish failover.

IT began to develop an Information Technology Service Management (ITSM) program to engender a change in IT delivery from one of providing technology to providing services. Funding and staffing constraints have led to this program being placed on hold through FY25.

Part of the ITSM program is the development of an IT Service Catalogue which includes cost transparency to the level of cost per unit of service provided. While some work has been completed in that area, it is not yet mature. A Major consideration is the cost for providing business resiliency for IT systems. We do that as a general principle for localized redundancy, and geographically for Critical Business Systems. However, for Enterprise Business Systems, IT has been relying on the agency Business Resiliency efforts to identify and prioritize system requirements in this area. Once completed, we can determine the cost of providing such services geographically.

8.5 Performance and Practices Benchmarking

In FY2012, IT joined a consortium of twenty utilities, UNITE, which engaged in benchmarking IT performance; however, due to cost constraints, IT dropped out of UNITE in mid-cycle of FY2016 benchmarking after completing only two bi-annual cycles of benchmarking (FY2012 and FY2014). Due to reductions in staff, IT has not engaged in formal benchmarking activities since then.

The FY2014 UNITE benchmarking provided some insight into IT performance relative to its peers in the utility space. Below is a comparison between BPA IT performance and the median UNITE performance values with some comments on what the comparisons may imply.

Table 8.4-1 FY2014 Performance Comparison with Utility Peers

Metric	FY2014 BPA IT	UNITE Median	Comments

Cost per End User Computing	$3,467	$1,273	BPA's lack of standardization, automation, and personalized high touch has resulted in BPA IT underperforming compared to 2014 UNITE's median. These factors were the drivers behind the BPA desktop virtualization (VDI) project. BPA is also investigating role-based provisioning and software title standardization to help improve reliability and reduce support costs.
End Users per support staff	241	805	
Cost Personal Computing Device per User	$1,560	$824	
Cost per End User Contact	$15.58	$11.49	
Average End User Contacts per Year	14.4	11.7	
Network Spend per End User	$1,154	$5,907	BPA has underspent compared to its peers. This underspend resulted in the need to launch a major network refresh project in FY2014 which completed in FY2017. Network gear are now being refreshed based on published refresh rates, see Table 7.4-2.
Cost per Wintel O/S	$5,606	$4,410	BPA IT completed a consolidation and virtualization project in FY2016. The last of BPA's legacy systems are being migrated to this environment. Once the migration is complete, the expectation is that performance will improve and possibly surpass the UNITE median. BPA IT is continuously working to achieve efficiencies through automation and enhanced monitoring.
Wintel O/S per support Staff	48.5	60.2	

9.0 RISK ASSESSMENT

Asset risk management is a disciplined approach for anticipating and avoiding events which have the potential to adversely affect program goals and strategic objectives. For consistency, five categories of risk have been identified and are analyzed in each asset program. Strategies to reach future state objectives are assessed against each risk category in order to create an optimum strategy that mitigates risk.

IT is not particularly adept at mature risk management from a general business perspective, but rather at a technical level in terms of cyber security and infrastructure and application up-time (reliability). Financial risks are less under our control and therefore more troublesome.

Risks: These are defined in accordance with the current Agency risk assessment categories to quantify their impact on operations if they are realized.

- **Safety:** Risks related to events that include acts of nature (fire, flood, storms, and earthquakes), accidents, theft, vandalism, terrorism, compliance with life safety codes, OHSA requirements, and building codes.
- **Reliability:** Risks that lead to the break-downs in the operations of people, processes, and/or systems due to asset failures and create potential for failure of utility controlled generation, transmission, or operations.
- **Financial:** Risks that have adverse effect on the execution of program initiatives in alignment with planned spending levels and escalating operations and maintenance costs due to asset condition.
- **Environmental:** Risks associated with adverse effects to local and regional environments caused by asset operation and maintenance.

- **Compliance:** Risk related to regulatory changes, lapses in compliance with, and noncompliance with regulatory and security requirements.

The following agency 5x7 framework underlies the identification of risk, likelihood, and consequence used to characterize IT risks.

Table 9.0-1 Risk Framework

	SAFETY	RELIABILITY	FINANCIAL	ENVIRONMENTAL	COMPLIANCE
Impact Level	The potential impact of a risk even on a public or worker safety	The potential impact of a risk even on service or grid reliability	The potential risk event resulting in a financial costs to customers/rate payers measured in incremental dollar impact	The potential impact on natural resources such as air, soil, water, plant or animal life	The potential impact of noncompliance with federal, state, local, industrial, or operational standards or requirements
Catastrophic	Many Fatalities, Mass Serious Injury or Illness: Many fatalities of employees, public members or contractors; Mass serious injuries or illness resulting in hospitalization, disability or loss of work; Widespread illness caused typically caused by sustained exposure to agents.	Customer Hours Impact: Outage resulting in greater than 20 million total customer hours of interruption.	Impact > $3 billion in costs; consider costs to customers, shareholders and third parties.	Irreversible and immediate damage to surrounding environment (e.g. extinction of species).	NonCompliance Impact: Actions resulting in potential closure, split or sale of Company.
Severe	Few Fatalities, Serious Injuries or Illness; Permanent Disability: Few fatalities of employee, public member or contractor; Many serious injuries or illnesses resulting in hospitalization, disability or loss of work; Localized illness typically caused by acute or temporary exposure to agents.	Outage resulting in at least 2 million total customer hours of interruption.	Impact between $300 million and $3 billion in costs; consider costs to customers, shareholders, and third parties.	Resulting in acute longterm damage greater than 10 years;Severe damage to surrounding environment.	NonCompliance Impact: Regulator issued cease and desist orders; Regulators force the shut down of critical assets, and demand changes to operations/administration
Extensive	Serious Injuries or Illness; Permanent Disability: Serious injuries or illness to many employees, public	Outage resulting in at least 200,000 total customer	Impact between $30 million and $300 million in costs; consider costs to customers, shareholders, and third	Resulting in significant mediumterm damage greater	NonCompliance Impact: Regulatory investigations and enforcement actions, lasting longer than a year; Violations that result in multiple large nonfinancial
pact: Significant new and updated enacted as a result of an event; ult in adopting modest changes to istration; Increased oversight from regulators.	Major	Serious Injuries or Illness; Permanent Disability: Serious injuries or illness to few employees, public members or contractors resulting in hospitalization, disability or loss of work; Several employees, member of the public or contractors sent requiring treatment beyond first aid.	Outage resulting in at least 20,000 total customer hours of interruption.	Impact between $3 million and $30 million in costs; consider costs to customers, shareholders, and third parties.	Resulting in moderate mediumterm damage greater than few months; Reversible damage to surrounding environment.	NonCompliance Im regulations are Violations that re operations/admini
Impact: Violations that result in o operations/administration; No oversight from regulators.	Moderate	Minor Injuries or Illness: Minor injuries or illness to several employees, public members or contractors; Few employees, member of the public or contractors requiring treatment beyond first aid.	Outage resulting in at least 2,000 total customer hours of interruption.	Impact between $300k and $3 million in costs; consider costs from customers, shareholders, and third parties.	Resulting in moderate shortterm damage of few months; Reversible damage to surrounding environment with no secondary consequences.	NonCompliance minor changes t additional
mpact: Selfreported or regulator entified violations.	Minor	Minor Injuries or Illness: Minor injuries or illness to few employees, public members or contractors requiring first aid.	Outage resulting in at least 200 total customer hours of interruption.	Impact between $30k and $300k in costs; consider costs to customers, shareholders, and third parties.	Immediately correctable damage to surrounding environment.	NonCompliance id
pact: No compliance impact up to dministrative impact.	Negligible	No injury or Illness.	Outage resulting in less than 200 total customer hours of interruption.	Impact of less than $30k in costs; consider costs to customers, shareholders, and third parties.	Resulting in negligible to no damage; Very small damage scale, if not negligible.	NonCompliance Im an a

Table 9.0-2 identifies IT risks in the five categories, along with their likelihood and consequence as defined by the framework, followed by heat maps to provide graphical representations. IT has more interaction with reliability, financial, and compliance, and less with safety and environment.

Table 9.0-2 IT Risk Assessment

Risk Category	Risk Name: Risk Description	Likelihood	Impact
Reliability	**Cyber Threat:** There are a number of cyber threat risks including attack threats from inside and outside BPA as well as different methods or vectors of attack. Risks include the operation of equipment with known and unknown vulnerabilities to cyber-attack. There are also programmatic or process risks, such as the lack of specific targeted cyber security risk assessments at the individual IT device level (DOE RMP Tier 3 level of risk management). These risks have been documented in the Cyber Security Strategic Plan.	Almost Certain	Major
Reliability Financial	**Cloud Adoption Impedance:** Combination of: • Incomplete understanding of interface complexities, dependencies, and/or business value. • The inability to acquire cloud computing architecting and management skills for the IT workforce or for the existing workforce to adapt to the requisite cloud management philosophies. Leads to: • Failing to develop/adopt cloud native solutions resulting in increased cloud migration risks and costs. • Slow adoption of cloud-based solutions resulting in end user dissatisfaction (end users attempt to contract SaaS outside of J with an associated increase in security risks and costs).	Almost Certain	Moderate
Financial	**Inadequate Benefit Tracking**: Business not managing (tracking and maintaining) business benefits leads to failure to program upgrades and/or replacement to restore positive Agency business value (business value exceeds cost to maintain and enhance system).	Almost Certain	Minor
Compliance Reliability	**Cyber Posture**: A new understanding of cyber risk appetite from leadership at the national, Departmental or BPA level results in the need to mitigate known or yet-to-be-identified weaknesses in our cyber security posture and/or new regulatory compliance requirements or substantially different interpretation by WECC of how to implement known and anticipated regulatory compliance.	Likely	Major
Reliability	**Aging Systems**: Maintaining aging and EOL systems from a lack of understanding of the decreasing value of legacy equipment and systems leads to increased maintenance costs and decreased ability to achieve planned cost efficiency and security improvements.	Likely	Major
Reliability Financial	**Technology Adoption:** Adoption of disruptive and emerging technology and evolving industry best practices (i.e., cloud-based services, managed services, etc.) may lead to tension, poor adoption of new practices, dissatisfaction, demoralized staff, and fear among staff accustomed to and satisfied with status quo.	Likely	Moderate
Compliance Financial Reliability	**Shadow IT**: Business subscribing to services without IT involvement (failing to adhere to BPA 473-1 and lack of compliance to OMB A-130) leads to potential exposure of BPA information and/or loss of data integrity (information security risks), damage to BPA reputation, contractual/legal issues, and cost overruns.	Possible	Major
Reliability Financial	**General Business System Resiliency**: Failure to define and characterize business system Resiliency leads to exposure to extended general business system outages during disaster scenarios.	Possible	Extreme
Financial	**Oracle License**: Loss or major modification of J's years-old concurrent user-based Oracle licensing agreement due to requiring new database capabilities not included under the current licensing agreement would require BPA to move some or all of its Oracle licensing to processor-based licensing leading to adding millions in net new annual maintenance expense costs to the IT budget.	Possible	Extreme
Environment/Trustworthy/ Stewardship	**User Satisfaction**: Unmet user expectations, driven by commercialization of IT, leads to user expectations that BPA will procure and provide IT support for similar personally-owned devices for business resulting in decreased user satisfaction and that pose unanticipated security and budgeting challenges.	Possible	Moderate
Financial Reliability	**Job Market:** The IT job market and unemployment in the northwest, coupled with a lack of support for remote work leads to: • Much higher expense costs in the IT budget to obtain and retain staff. • Inability to attract appropriate skill levels.	Almost Certain	Moderate
Safety Reliability	**On-the-job Injuries:** IT workers are injured while in duty status due to: • Travel accidents • Slips, trips, or falls • Installation of electronic IT equipment	Possible	Minor

Risk Category	Risk Name: Risk Description	Likelihood	Impact
	• Repetitive ergonomic maladies Leads to: • Insufficient staff to meet operational requirements • Delays to project schedules resulting in lower financial benefits		
Financial	**Contract Inflation:** Maintenance contracts for IT products and services continue to outpace national economic inflation rates leading to increased cost pressure on IT expense budgets.	Almost Certain	Major
Reliability Financial Compliance	**Malware Threats:** The proliferation of Cyber-attacks through multiple vectors continues to drive faster adoption of security fixes, and a rise in governmental mandates to implement specific cyber security architectures and practices, and to respond to ever-increasing data calls, leading to increased cost of operating information technology functions.	Almost Certain	Moderate
Compliance Financial	**Technology Directives:** New Federal directives or orders that require the implementation of specific information technology architectures and/or systems, leading to increased IT budget pressures for products, contracts, and support personnel (e.g. IPv6, WECC security, Continuous Diagnostics and Mitigation, Zero Trust Architecture).	Almost Certain	Moderate

The following heat maps illustrate the five risk assessment categories.

Figure 9.0-1, Risk Assessment, Safety

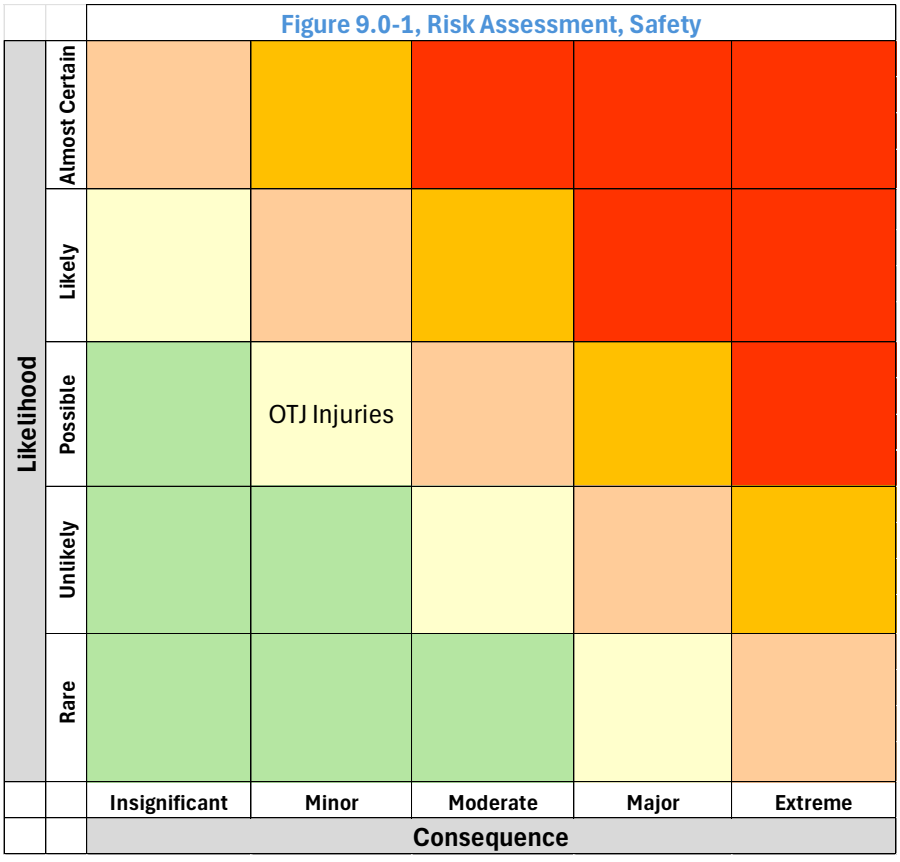


Figure 9.0-2, Risk Assessment, Reliability

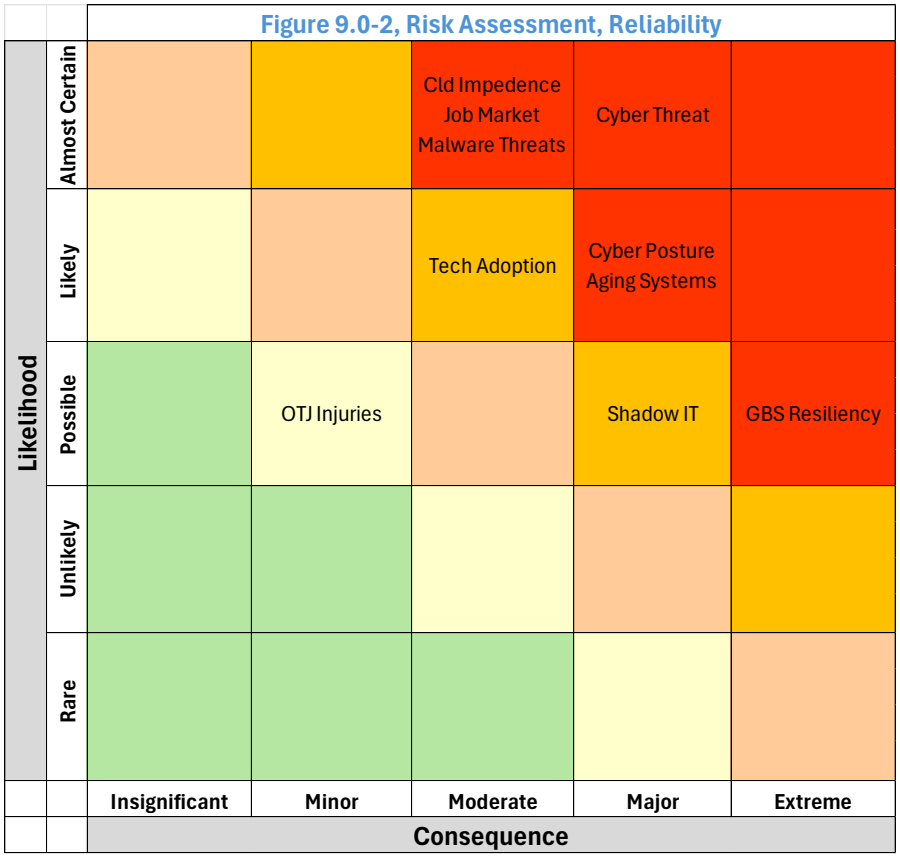


Figure 9.0-3, Risk Assessment, Financial

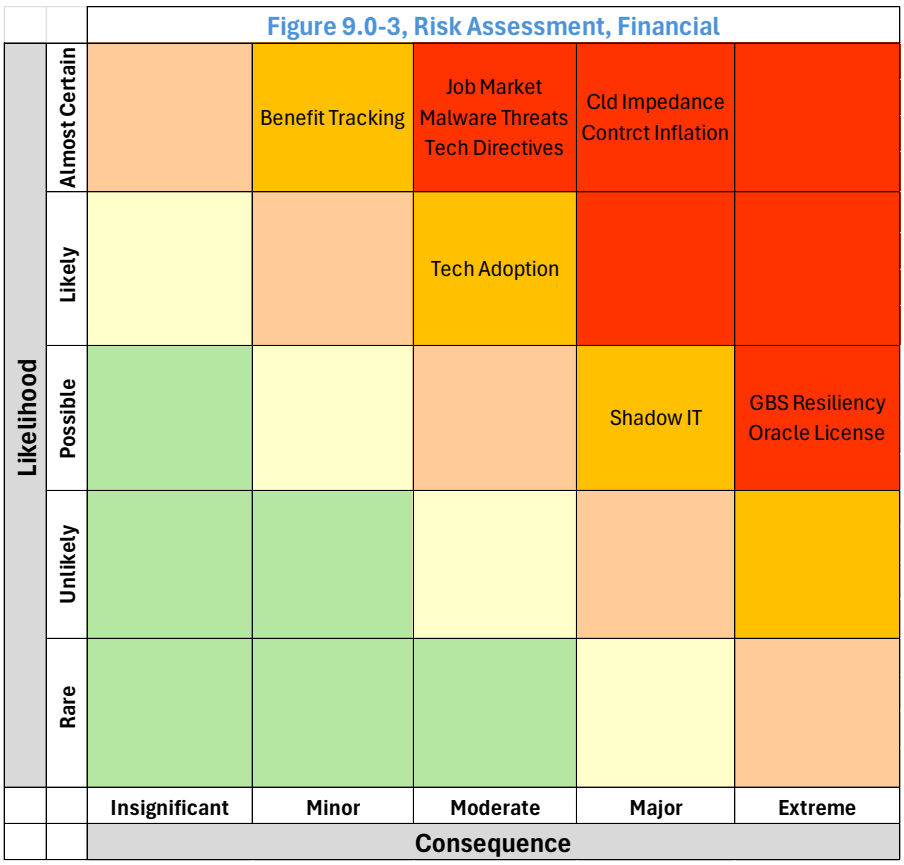


Figure 9.0-4, Risk Assessment, Environmental

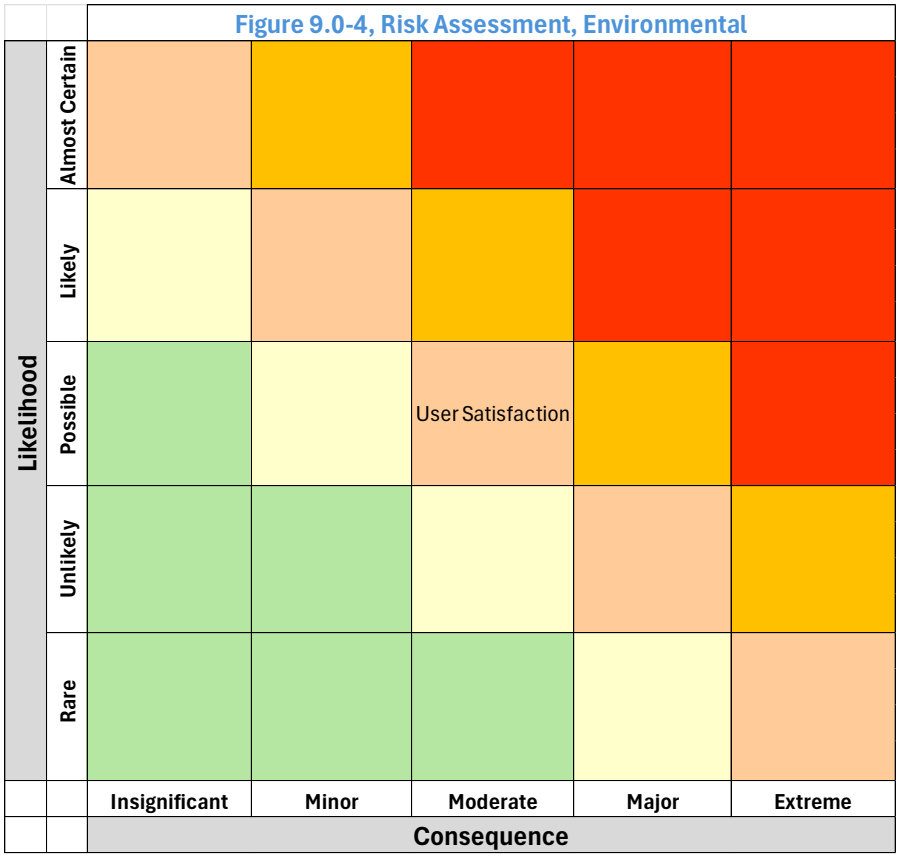
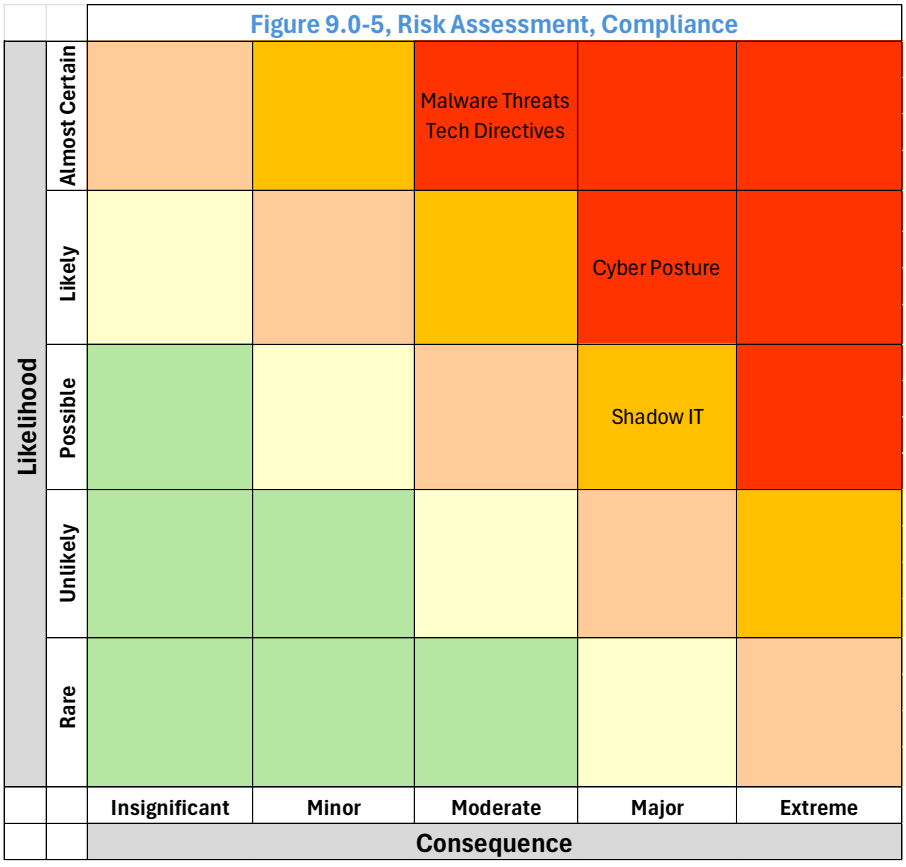


Figure 9.0-5, Risk Assessment, Compliance



10.0 STRATEGY AND FUTURE STATE

The IT SAMP addresses two distinct set of assets, infrastructure and business applications, with separate characteristics and objectives. Infrastructure assets include all information devices and management software needed to provide connectivity, computational capacity, and electronic storage, as well as the management software needed to host, operate, and secure applications to meet the business automation needs of BPA. The infrastructure consists primarily of standardized physical devices with accepted industry refresh rates. The business application assets consist of intellectual property from a multitude of vendors, each with their own tempo for upgrades and support cycles. Retaining existing applications and placing new systems into production is driven primarily by evolving business needs.

Since 2018 and through FY25, IT will have labored under limited funding to contribute to BPA's flat rate obligation. IT has reduced staff, contractual obligations where feasible, and deferred customer demand, to attempt to meet budget requirements while continuing to operate and maintain a large portfolio of IT assets. As a result, we have begun to experience increasing system outages and time to recover, all but exhausted our ability to provide new systems for our customers, and begun to fall behind regulatory compliance requirements. The staff that performs operations and maintenance for IT assets is the same staff that performs enhancements and brings in new systems to the agency. This has contributed to the deferral of life cycle activities for existing products and services in some cases, in favor of adding new important BPA business capabilities such as Grid Modernization and Energy Imbalance Market.

To address these issues, the overall strategy for IT over the next several years is to focus on modenization of digital systems and IT business processes, including maturation of IT asset management and improving safe and reliable system operations through a culture of compliance and improved resiliency of IT systems. Driven by the most important risks identified earlier, this includes IT organizational stability resulting from focused staff planning and restoration. IT will develop and pursue the following high-level strategy initiatives to meet these objectives:

- Business Readiness – Establish process for analysis and improvement of customer readiness for new technology solutions.
- Business and IT Service Planning - Develop business processes for IT customers to collaborate with IT on the development of IT services.
- BPA Business Initiatives for Corporate Modernization, Market Plus, and Day Ahead – Collaborate with the Business Transformation Office to work with business line customers to define and plan these business initiatives.
- Enterpirse Asset Management Maturity - Mature asset management capabilities across BPA.
- Cloud Adoption – Expand and mature an IT Cloud Strategy.
- IT Service Planning and Transparency Capability Improvement - Provide our internal customers visibility into the costs and performance of IT products and services.
- IT Demand Management – Develop policy and process for effective executive prioritization for customer IT requests.
- IT Stabilization and Get Well Plan - restore specific core IT service levels.
- IT Asset Life Cycle - maximize IT asset lifecycle, from initial deployment to responsible end-of-life services, including minimizing technical debt as much as feasible.
- IT Service Management Adoption – Select a service management framework for monitoring and managing IT service delivery.
- Enterprise IT Modernization – Re-establish an Office of the Chief Technology Officer (OCTO) with dedicated R&D resources

- Cybersecurity Program and Compliance – Develop a roadmap to enhance BPA's Cybersecuirty Program to ensure it meets all compliance requirements.
- Continuous Diagnostics and Mitigation – Implement, operate, and maintain this federal requirement.
- Zero Trust Architecture – Develop a roadmap for compliance with this federal requirement.
- IT Security Operations Center - centralize, standardize, and coordinate operational security across all of BPA's J enterprise IT organizations, environments, and systems.
- IT Separation of Development and O&M Duties – Improve maintenance and security of BPA's IT software environment, and eliminate the conflict between development of project solutions and support of existing systems.

Capital sustain replacements for hardware in the data center and network portfolios have eliminated those backlogs recently, and the implementation of desktop equipment leases has eliminated backlogs for hardware in the office automation category. There remain some backlogs in expense sustain efforts that will be identified in the current asset inventory refresh, and likely some impending capital and expense sustain replacements that will also be identified for the applications portfolio. Once identified, these backlogs are expected to be addressed through the IT Stabilization and Get Well Plans strategic initiative.

10.1 Future State Asset Performance

Key measures were introduced in Section 8.3 as the desired IT asset health indicators. Reaching green for each indicator are the IT asset performance future objectives.

Table 10.1-1 Future Asset Performance Objectives

Objective	This Year	Year +1	+2	+3	+4	+5
System Reliability	95%	97%	98%	98%	98%	98%
System Financial Value	90%	91%	92%	93%	94%	94%
System Business Needs	90%	92%	95%	95%	95%	95%
Security & Risk	92%	94%	97%	97%	97%	97%
System Resiliency	40%	60%	80%	90%	98%	98%

Two major outcomes are expected from these performance objectives:

- Evolving the infrastructure to meet emerging security threats and providing reliable services while lowering operation and investment costs.
  - Security and Risks
  - Reliability
  - Resiliency

- Meeting strategic and emerging business needs by providing business solutions that deliver demonstrable positive net value and benefits to the Agency and the Northwest.
  - Business Needs
  - Financial Value

The first major outcome is more easily defined and measured based on age and version characteristics of individual assets, and whether or not they have continuous operations capabilities. As described earlier, this type of inventory information is in the process of being refreshed at this time. The second major outcome is not yet well defined and will require development and execution plans, with resources, to become meaningful.

10.2 Strategy

The following sections describe the IT strategies for sustainment of and new demand for IT products and services with the intent to provided enough information to enable the development of specific IT Asset Plans.

10.2.1 Sustainment Strategy

Table 10.2.1-1 provides the current industry/vendor best practice refresh cycles for infrastructure components and applications. While the infrastructure information is fairly solid, software vendors tend to vary somewhat on the application life expectancy and upgrade paths. However, diligent application of these lifecycle refreshes will increase the reliability and security measures to the expected levels.

Table 10.2.1-1 Major Component Types and Characteristics

Major Component	Characteristics	Life Expectancy	Operation & Maintenance Standards
Servers	Refresh using industry/vendor best practice of 3 years for IT hardware	3 years	Time based maintenance
Storage (SANs and Fabric)	Refresh using industry/vendor best practice of 3 years for IT hardware	3 years	Time based maintenance
Desktops	Refresh using industry/vendor best practice of 3 years for IT hardware	3 years	Time based maintenance
Laptops	Refresh using industry/vendor best practice of 3 years for IT hardware	3 years	Time based maintenance
Thin Clients	Refresh using industry/vendor best practice of 6 years	5-7 years	Time based maintenance
Tablets	Refresh using industry/vendor best practice of 3 years	3 years	Time based maintenance
Plotters	Refresh using industry/vendor best practice of 3 years for IT hardware	3 years	Time based maintenance

Network devices	Refresh using industry/vendor best practice of 5 years	5-7 years	Time based maintenance
Smart Phones/Wireless devices	Refresh using GSA's Federal Strategic Sourcing Initiative (FSSI) on wireless to use latest smartphone mobile that vendors offer free under their contact	2-3 years	Time based maintenance
Software Systems	Refresh/upgrade to maintain software within N-1 of vendor's current version to ensure operational reliability and security	4 years	Achieving business value, meeting business needs, and staying within N-1 of current vendor supported version (security/reliability)

Using an annual percentage refresh cycle for data center and network assets allows IT to rotate equipment to the failover function, then test, then development environments. IT also stocks 10% spares for speedy replacement of unexpected hardware failures, and utilizes vendor maintenance contracts for hardware that is more specialized. Office automation equipment uses a lease strategy to contractually replace those assets on a three-year rotation with one third of the fleet replaced each year. There are also some spares, loaners, and temporary workstations deployed to meet individual emergency situations. This sustainment rotation and sparing enables the security and risks, reliability, and resiliency objectives for most if not all systems from an infrastructure perspective.

The applications portfolio is more complex due to the number of dependencies and integrations between the various information systems, and the propensity for cyber security threats to target software. This can require extensive testing and extended time periods to execute upgrades or replacements. The IT strategy for larger and more complex changes is that they must be planned and executed with care using the disciplines defined within BPA's System Life Cycle processes and requirements, utilizing the expertise of business analysts, project managers, technical leads, information owners, business subject matter experts, etc. in a well-defined framework. Complicating matters for resiliency is that many software systems are not designed for failover, and maintaining duplicate copies of large volumes of data is complex and problematic. IT's strategy in this area is to attract and retain related skillsets and augment with vendor-provided expertise where needed, to provide optimal solutions based on individual software characteristics. A developing strategy is to shift these responsibilities to cloud-based solution providers in cases where risks are sufficiently mitigated to allow off-site processing and total costs remain equivalent or lower.

The objectives of meeting business needs and financial value can only be determined by the business units that use the systems, with the latter needing IT to provide the cost of maintenance (labor plus maintenance/support contracts). At each system refresh lifecycle event, this information should be used to inform the decision of retire or replace or upgrade the system, based on whether or not the system is meeting defined business needs and the value provided is greater than the cost to maintain the system (as long as there is no compliance aspect to the requirements). The primary obstacles to addressing these objectives is that the business units do not understand how to measure them or do not have resources to perform that tracking, and lack of IT resources to guide and assist with that tracking. Service and resource improvements identified in some of the IT strategies in section 10 will enable these objectives within this IPR cycle.

The process and method for prioritizing sustain projects is not expected to change from what was described in section 7: Sustain prioritized over expand, Critical systems before Enterprise systems, Reliability and Compliance before Discretionary, etc. All major efforts must still stand before the APSC for final prioritization and recommendation to the CIO, and are tracked by the APSC through the various stage gates described in the System Life Cycle.

10.2.2 Growth (Expand) Strategy

IT's goal is the efficient deployment of Information Technology to promote the economically efficient use of technology in meeting BPA's business requirements. Without the IT Client's direct responsibility and accountability for making the case for tangible business value, we cannot effectively estimate or even measure the business value of IT products and services. In order to increase the level of engagement of business clients in the management of IT assets, IT has deployed Strategic Business Partners to each of the main business lines at BPA: Power, Transmission, and Corporate. The Strategic Business Partners maintain a collaborative relationship with IT's business lines to improve or achieve the following:

- Assist the business information owners and sponsors to take an enterprise architecture approach to solving business problems. This includes business process evaluation and re-structuring before turning to automation solutions.
- Assist the business information owners and sponsors to determine and subsequently measure the business value of Expand IT projects, to promote effective and efficient use of technology.
- Develop and/or support existing bodies within the business lines to collect and prioritize their IT projects with a view to longer range planning. These will then be forwarded to the IT Intake Process for initial scoping validation and then to the Agency Priority Steering Committee for cross-agency prioritization and tracking.

In conjunction with this effort, the System Life Cycle processes used for IT projects is adding a stronger emphasis on ensuring that future expense budgets will be dedicated to support (net new O&M) those additional applications once they have been installed.

As outlined in section 7, the process and method for prioritizing expand projects is not expected to change: sustain before expand, Critical systems before Enterprise systems, Reliability and Compliance before Discretionary, etc. All major efforts must still stand before the APSC for final prioritization and recommendation to the CIO, and will be tracked by the APSC through the various stage gates described via the System Life Cycle.

10.2.3 Strategy for Managing Technological Change and Resiliency

Technological Change

Technological changes are expected, and in fact do, arise between life cycle refresh events for IT assets. The speed of IT technological change dictates that this will occur. However, any changes in the assets prior to the proscribed refresh cycles must provide a robust business case that includes a positive net financial gain, and meets real business needs in order to be considered for pre-refresh execution.

The Cybersecurity program is currently adding resources to increase its capacity to evaluate automated systems' Authority to Operate (ATO), which includes the related System Security Plans. This will identify shortcomings in cyber security posture for those systems and initiate life cycle activities to correct them. In addition, since the last SAMP period

the Office of the CIO has implemented a strategy that employs an IT Procurement Coordinator to track and report on compliance with FISMA and FedRAMP requirements that are now included in IT purchasing processes.

Resiliency

IT has long been supporting various levels of resiliency within it's portfolio. The first layer is redundancy of local facilities: dual path power to equipment, emergency generators with UPS switching, and multiple cooling units. IT equipment itself is architected with multiple power supplies, multiple processing units, electronic storage and memory that withstand component failures, and multiple paths to storage and internet connections. Some software systems support multiple functional levels for load sharing (web farm, application farm) that absorb losses of identical units. IT's Critical Business Systems were designed with the ability to failover to geographically separate facilities some time ago, undergoing annual verification testing, and those techniques will be applied to other systems over time.

As described in section 10.2.1, the sustain strategy contains provisions for adding resiliency for the Enterprise Business Systems by using a life cycle rotation to provide resources in the alternate data center in Munro to host failover. While this sounds simple, it is not. Solutions to provide failover capability for the Enterprise Business Systems must be tailored somewhat for each system and include considerations for:

- Facilities power and cooling capabilities.
- Ability for specific applications to be failover-aware, to relocate operating environments with a minimum of human intervention.
- Determination for use of cloud-based failover as opposed to our existing alternate data center, including disposition of data integration methods both between on-premise and cloud-based systems, and between cloud-based systems.
- Staging and integrity of data storage between different locations.

The technological architecture of the software systems and infrastructure to support them must be orchestrated in such a way as to minimize downtime for the necessary changes and verification testing, and take into account the inter-system dependencies that have developed over time. Several of the high-level strategies enumerated at the beginning of this section positively impact the resiliency posture of the IT asset portfolios, including Continuous Diagnostics and Mitigation, Zero Trust Architecture, Cloud Adoption, IT Asset Life Cycle, and Enterprise IT Modernization.

Additionally, IT added a skilled resource for the identification, documentation, planning, and testing of contingency plans for automated business systems prior to this SAMP cycle. This resource is working with BPA's Continuity Office and various Information Owners to establish appropriate requirements and measurements for IT's continuity and resiliency programs.

Sustainability and Climate Resilience

IT already utilizes multiple network paths to our physical assets in field locations and data centers, enabling our strategy for geographical redundancy and failover. This provides the solid foundation of network communications that must be in place to successfully execute on BPA's mission, even in the face of localized events triggered by extreme climate-related conditions. Our remote work capabilities deployed a few years ago have already proven to be capable and adequate for supporting the entire BPA workforce in a maximum telework posture. Furthermore, our strategy of maintaining spares for key pieces of the infrastructure mitigates temporary disruptions of supply chain delivery.

Climate change threats are more likely to affect building plant assets, and IT relies on the Facilities organization to maintain those assets in working condition through threat events, providing adequate power and cooling to operate IT assets.

10.3 Planned Future Investments/Spend Levels

IT continues to have a strong sense of the sustain funding required to maintain those assets that are already in production. BPA's recent years of holding expense funding at a very low level has curtailed IT's ability to meet new customer demand and at the same time maintain existing systems and manage economic inflation related to goods and services. This has resulted not only in lower asset performance (more system outages), but created a long list of both work efforts to regain acceptable health levels and a growing backlog of pent-up customer demand. And, historical experience indicates that IT's business line partners often generate requests for major application expansion efforts on a much shorter timeframe than the three years and beyond examined during the IPR process. This requires IT to be somewhat dynamic in planning for future investments. This SAMP period intends to recitify those issues by including a right-sized staff to adequately perform the required operations and maintenance activites for existing systems, augment staff to improve IT business operations and customer service and planned increases in cross-agency personnel, and meet a reasonable rate of new IT systems and capabilities to support business line strategic goals.

These changes in overall spending profile for IT, maintaining existing systems but also focusing on customer demand and quality, impact not only capital and expense requirements for implementation, but also create additional increases in core operations and maintenance budget requirement after project implementation. These costs must be identified and included in core budgets, and in fact are identified in the future spending forecasts contained in the tables below (Expense for O&M Tail, average of 8.2% of implementation cost). A good example of this is Zero Trust Architecture: compliance with federal directive, not well defined, and likely to be a large expenditure for both implementation and on-going maintenance and support.

There are additional pressures that influence the type of funding, capital or expense, that may be needed for any specific effort, and influence the shape of IT funding. For example, previous Federal guidelines were very strong on the use of cloud computing for future solutions, and those cloud-based solutions were to be totally expense. Recent Federal guidance tones down the requirement to use the cloud, and allows portions of that work to be capitalized. And vendors have reacted as well, providing creative ownership options that allow further capitalization of cloud solutions.

Since Tables 10.3-1 and 10.3-2 are for IPR exposure, the following assumptions should be noted:

1) Unknown capital expand project requests may still come from the business lines on fairly short notice. These must include consideration for expense funding as well (20% for implementation, 8.2% for annual net new O&M).
2) The expense profile includes net new O&M from in-flight projects in FY24 and FY25.
3) The Capital Sustain in 2028/29 includes expenditure for building out the new Vancouver Control Center building, and migrating the HQ data center there.
4) While we have no detailed information at this time, we expect an effort to modernize Corporate systems to begin in FY26 (CorpMod).
5) Underlying details that break down the components of the business line and IT Projects are presented in Appendix A.

Table 10.3-1 Future Optimal Expenditures (in thousands)

($ Thousands)	Rate Case FY's			Future Fiscal Years						
Capital (CapEx)	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Total Capital Sustain	10,460	10,941	11,444	16,759	17,530	18,337	19,180	20,062	20,985	21,951
Total Capital Expand	30,334	31,729	30,900	13,767	11,269	11,788	12,330	12,897	13,490	14,111
Total Capital (Sustain and Expand)	**40,794**	**42,671**	**42,344**	**30,526**	**28,800**	**30,124**	**31,510**	**32,960**	**34,476**	**36,062**
Expense (OpEx)										
PMO Expense	12,336	12,458	11,888	7,234	6,684	6,991	7,313	7,649	8,001	8,369
Total IT Expense	**197,295**	**212,678**	**220,811**	**231,852**	**243,444**	**255,616**	**268,397**	**281,817**	**295,908**	**310,703**
Total Capital & Expense	**238,089**	**255,349**	**263,155**	**262,378**	**272,244**	**285,740**	**299,907**	**314,777**	**330,384**	**346,765**

Table 10.3-2 captures the funding that we expect to be approved. Two specific efforts that make up part of the IT portfolio, IT Stabilization and Enterprise IT Modernization, are key enablers of the overall plan. Without them, IT wil be unable to staff back up to effectively service existing systems and customer requirements, nor will IT be able to achieve improvements in service and asset management delivery. They enable most of the other activities.

Table 10.3-2 Future Expected Expenditures (in thousands)

($ Thousands)	Rate Case FY's			Future Fiscal Years						
Capital (CapEx)	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Total Capital Sustain	10,460	10,941	11,444	16,759	17,530	18,337	19,180	20,062	20,985	21,951
Total Capital Expand	25,000	26,150	27,353	13,767	11,269	11,788	12,330	12,897	13,490	14,111
Total Capital (Sustain and Expand)	**35,460**	**37,091**	**38,797**	**30,526**	**28,800**	**30,124**	**31,510**	**32,960**	**34,476**	**36,062**
Expense (OpEx)										
PMO Expense	10,832	10,874	10,888	7,234	6,684	6,991	7,313	7,649	8,001	8,369
Total IT Expense	**195,791**	**211,105**	**219,811**	**230,802**	**242,342**	**254,459**	**267,182**	**280,541**	**294,568**	**309,296**
Total Capital & Expense	**231,251**	**248,196**	**258,608**	**261,328**	**271,142**	**284,583**	**298,692**	**313,501**	**329,044**	**345,358**

10.4 Implementation Risks

Table 10.4-1 presents some implementation risks to operating the IT asset management strategy.

Table 10.4- Implementation Risks

Risk	Impact	Mitigation Plan
IT Service Catalogue Fails.	Customers cannot determine cost of IT services.	ITSM Program Manager is assigned to oversee the catalogue creation.
Supply Chain is unable to process purchases in a timely manner.	Replacements cannot be completed on schedule, resulting in slippage in asset performance objectives.	Work to get replacement purchases into the Supply Chain system early in the year.
IT service providers can't track cost per unit.	Service catalogue is rendered invalid.	Assign business analysts to assist IT service providers in creating repeatable cost calculators.
IT expense budget is inadequate to execute sustain activities.	Asset performace objectives will not be met, possibly leading to increased downtime and higher risk of cyber incursions.	Request additional expense funding to at least maintain current activities/refreshes with inflation. Move more equipment to lease contracts.

Inability to obtain/retain appropriate staff.	Asset performace objectives will not be met, possibly leading to increased downtime and higher risk of cyber incursions.	Work with the agency to offer remote work for IT positions, increase expense budget to account for scarcity in the IT job market, and increasing cost of labor.

10.5 Asset Conditions and Trends

Making sure that all sustain activities adhere to the proscribed life cycle refreshes will maintain all business function applications and all infrastructure in a healthy status, delivering reliable, safe, and valuable assets that meet business needs.

Inadequate expense funding for IT will result in insufficient staff to update applications on schedule, and insufficient capacity to keep maintenance contracts current. IT plans to seek additional funding levels beginning in FY24 IPR to address these shortcomings. In addition the IT Strategic Business Partners continue to work with the business lines to emphasize the importance of software remaining current and patched.

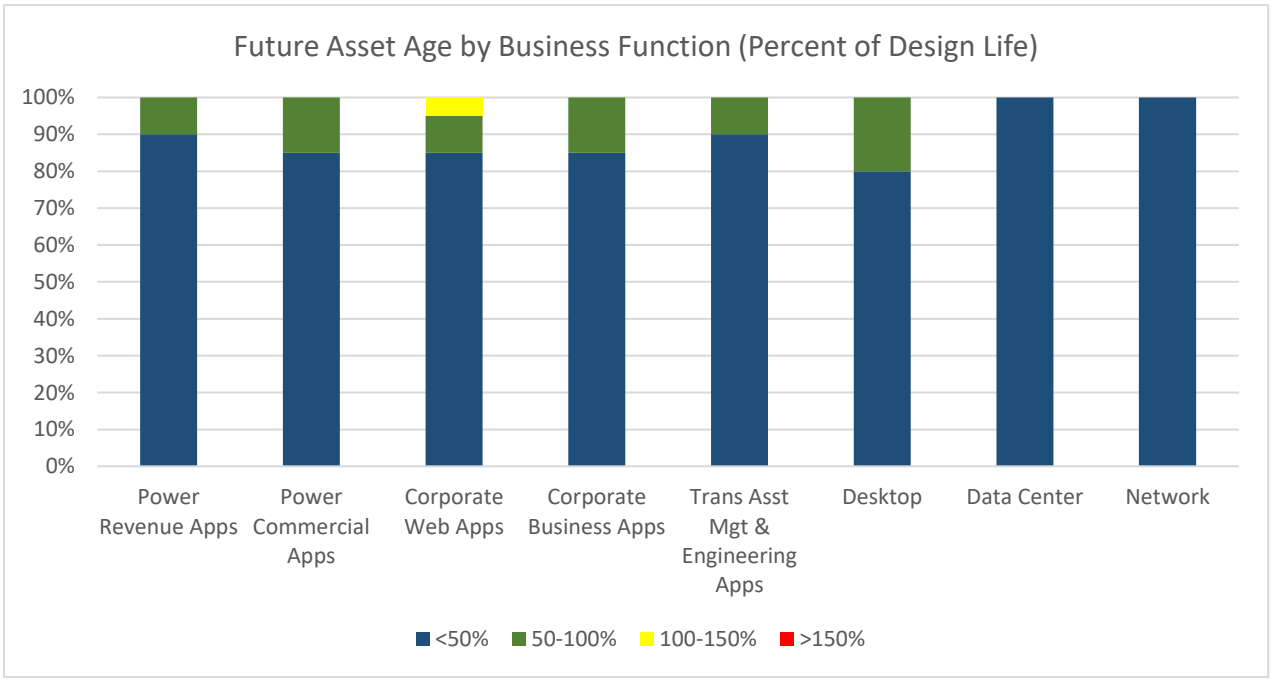


Figure 10.5-1 Future Asset Age by Business Function

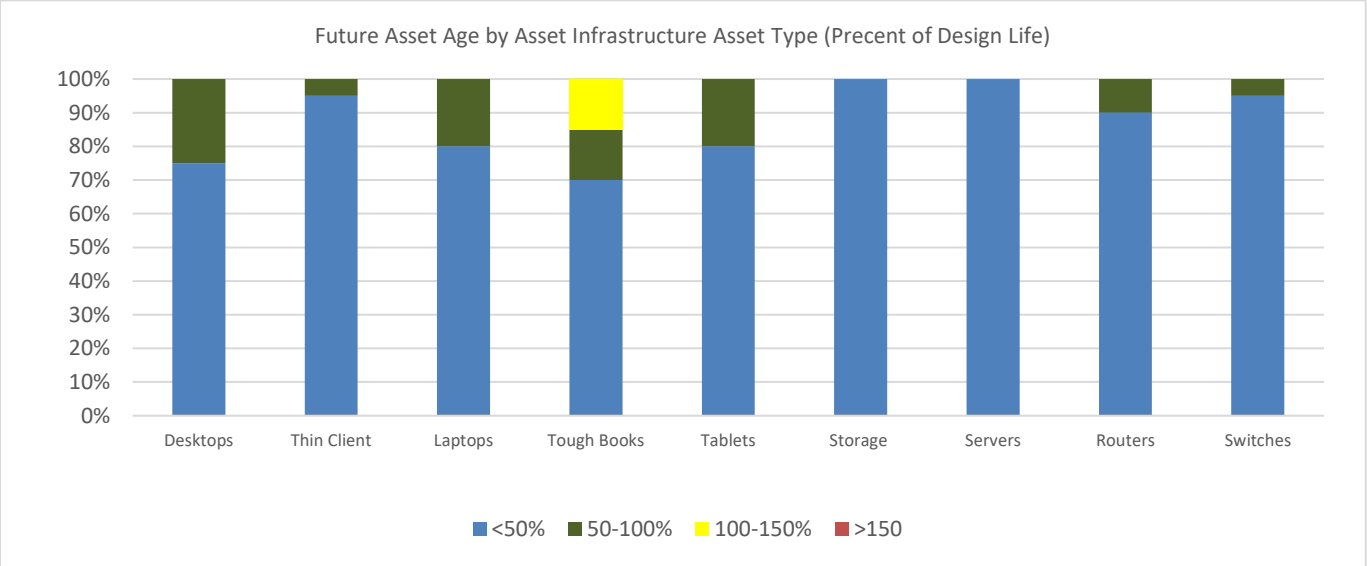


Figure 10.5-2 Future Asset Age by Asset Type

10.6 Performance and Risk Impact

Table 10.6.1 contains the same risks as identified in Section 9, but with updates to the risk likelihood and impact based on forecasted impacts of the various IT strategies.

Table 10.6-1 Strategy Impact on IT Risk Assessment

Risk Category	Risk Name: Risk Description	Likelihood	Impact
Reliability	**Cyber Threat:** There are a number of cyber threat risks including attack threats from inside and outside BPA as well as different methods or vectors of attack. Risks include the operation of equipment with known and unknown vulnerabilities to cyber-attack. There are also programmatic or process risks, such as the lack of specific targeted cyber security risk assessments at the individual IT device level (DOE RMP Tier 3 level of risk management). These risks have been documented in the Cyber Security Strategic Plan.	Almost Certain	Major
Reliability Financial	**Cloud Adoption Impedance:** Combination of: • Incomplete understanding of interface complexities, dependencies, and/or business value. • The inability to acquire cloud computing architecting and management skills for the IT workforce or for the existing workforce to adapt to the requisite cloud management philosophies. Leads to: • Failing to develop/adopt cloud native solutions resulting in increased cloud migration risks and costs. • Slow adoption of cloud-based solutions resulting in end user dissatisfaction (end users attempt to contract SaaS outside of J with an associated increase in security risks and costs).	Possible	Moderate
Financial	**Inadequate Benefit Tracking**: Business not managing (tracking and maintaining) business benefits leads to failure to program upgrades and/or replacement to restore positive Agency business value (business value exceeds cost to maintain and enhance system).	Likely	Minor

Risk Category	Risk Name: Risk Description	Likelihood	Impact
Compliance Reliability	**Cyber Posture**: A new understanding of cyber risk appetite from leadership at the national, Departmental or BPA level results in the need to mitigate known or yet-to-be-identified weaknesses in our cyber security posture and/or new regulatory compliance requirements or substantially different interpretation by WECC of how to implement known and anticipated regulatory compliance.	Unlikely	Moderate
Reliability	**Aging Systems**: Maintaining aging and EOL systems from a lack of understanding of the decreasing value of legacy equipment and systems leads to increased maintenance costs and decreased ability to achieve planned cost efficiency and security improvements.	Unlikely	Minor
Reliability Financial	**Technology Adoption:** Adoption of disruptive and emerging technology and evolving industry best practices (i.e., cloud-based services, managed services, etc.) may lead to tension, poor adoption of new practices, dissatisfaction, demoralized staff, and fear among staff accustomed to and satisfied with status quo.	Likely	Moderate
Compliance Financial Reliability	**Shadow IT**: Business subscribing to services without IT involvement (failing to adhere to BPA 473-1 and lack of compliance to OMB A-130) leads to potential exposure of BPA information and/or loss of data integrity (information security risks), damage to BPA reputation, contractual/legal issues, and cost overruns.	Unlikely	Moderate
Reliability Financial	**General Business System Resiliency**: Failure to define and characterize business system Resiliency leads to exposure to extended general business system outages during disaster scenarios.	Possible	Major
Financial	**Oracle License**: Loss or major modification of J's years-old concurrent user-based Oracle licensing agreement due to requiring new database capabilities not included under the current licensing agreement would require BPA to move some or all of its Oracle licensing to processor-based licensing leading to adding millions in net new annual maintenance expense costs to the IT budget.	Possible	Major
Environment/Trustworthy/ Stewardship	**User Satisfaction**: Unmet user expectations, driven by commercialization of IT, leads to user expectations that BPA will procure and provide IT support for similar personally-owned devices for business resulting in decreased user satisfaction and that pose unanticipated security and budgeting challenges.	Unlikely	Minor
Financial Reliability	**Job Market:** The IT job market and unemployment in the northwest, coupled with a lack of support for remote work leads to: • Much higher expense costs in the IT budget to obtain and retain staff. • Inability to attract appropriate skill levels.	Almost Certain	Moderate
Safety Reliability	**On-the-job Injuries:** IT workers are injured while in duty status due to: • Travel accidents • Slips, trips, or falls • Installation of electronic IT equipment • Repetitive ergonomic maladies Leads to: • Insufficient staff to meet operational requirements • Delays to project schedules resulting in lower financial benefits	Unlikely	Minor
Financial	**Contract Inflation:** Maintenance contracts for IT products and services continue to outpace national economic inflation rates leading to increased cost pressure on IT expense budgets.	Almost Certain	Major
Reliability Financial Compliance	**Malware Threats:** The proliferation of Cyber-attacks through multiple vectors continues to drive faster adoption of security fixes, and a rise in governmental mandates to implement specific cyber security architectures and practices, and to respond to ever-increasing data calls, leading to increased cost of operating information technology functions.	Almost Certain	Moderate
Compliance Financial	**Technology Directives:** New Federal directives or orders that require the implementation of specific information technology architectures and/or systems, leading to increased IT budget pressures for products, contracts, and support personnel (e.g. IPv6, WECC security, Continuous Diagnostics and Mitigation, Zero Trust Architecture).	Almost Certain	Moderate

Some risks, such as cyber threats and job markets, are not influenced by IT strategies. We can only prepare to react to them and that is already within our capabilities. However, there are several risks that the IT strategies will shrink in likelihood, consequence, or both. The most affected include cloud impedance, general business system resiliency, cyber posture, shadow IT, and aging systems. All of these are important aspects of IT asset health.

The following heat maps illustrate the five risk assessment categories after successful implementation of the IT strategies.

Figure 10.6-1, Risk Assessment, Safety

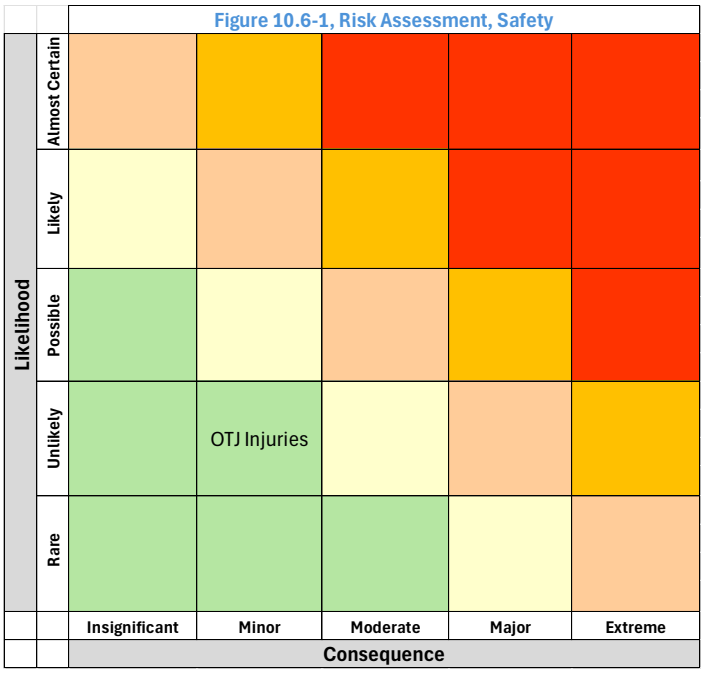


Figure 10.6-2, Risk Assessment, Reliability

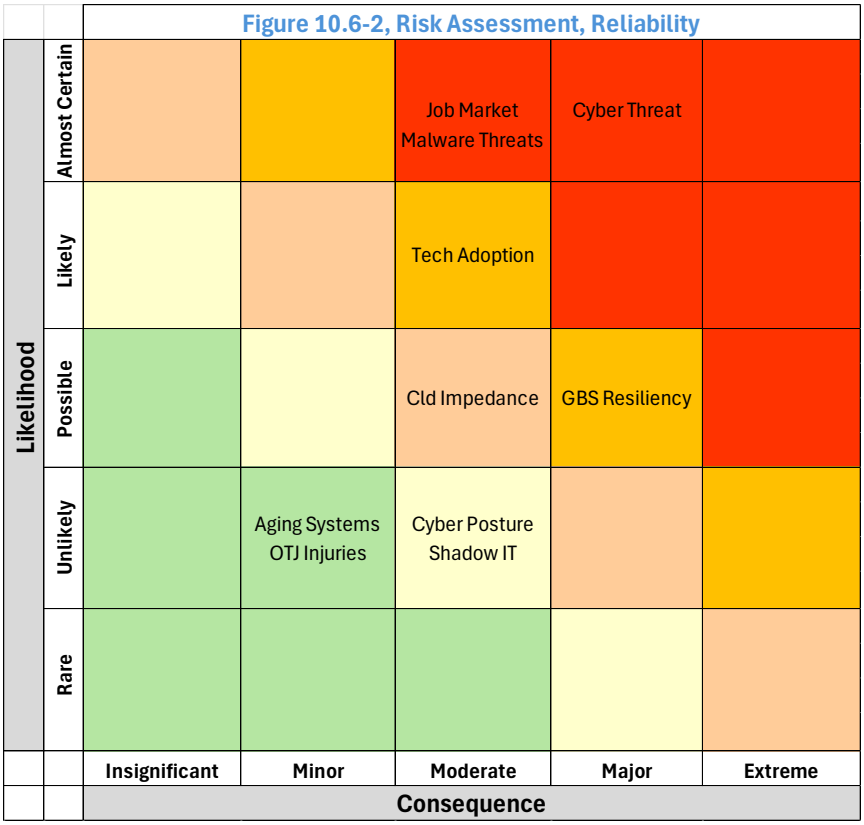


Figure 10.6-3, Risk Assessment, Financial

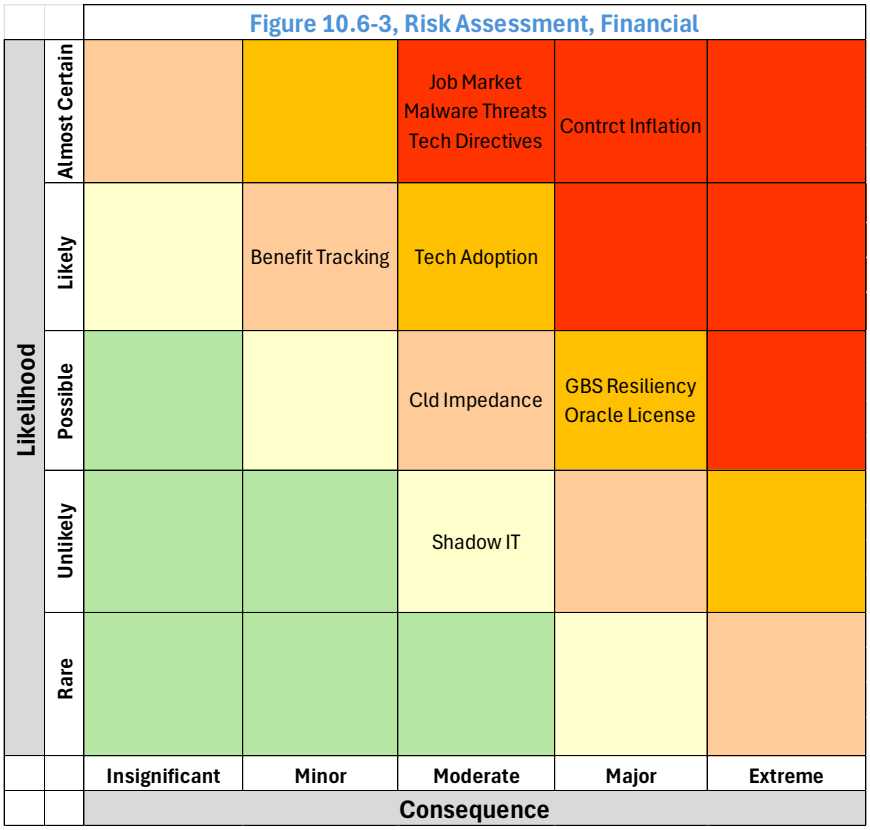


Figure 10.6-4, Risk Assessment, Environmental

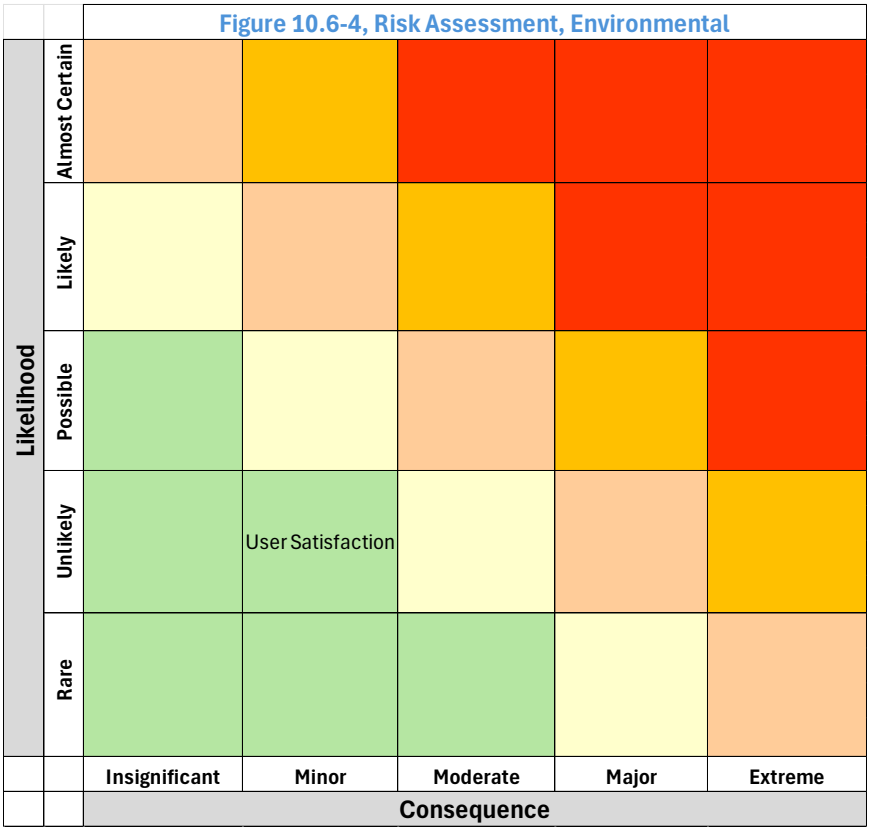
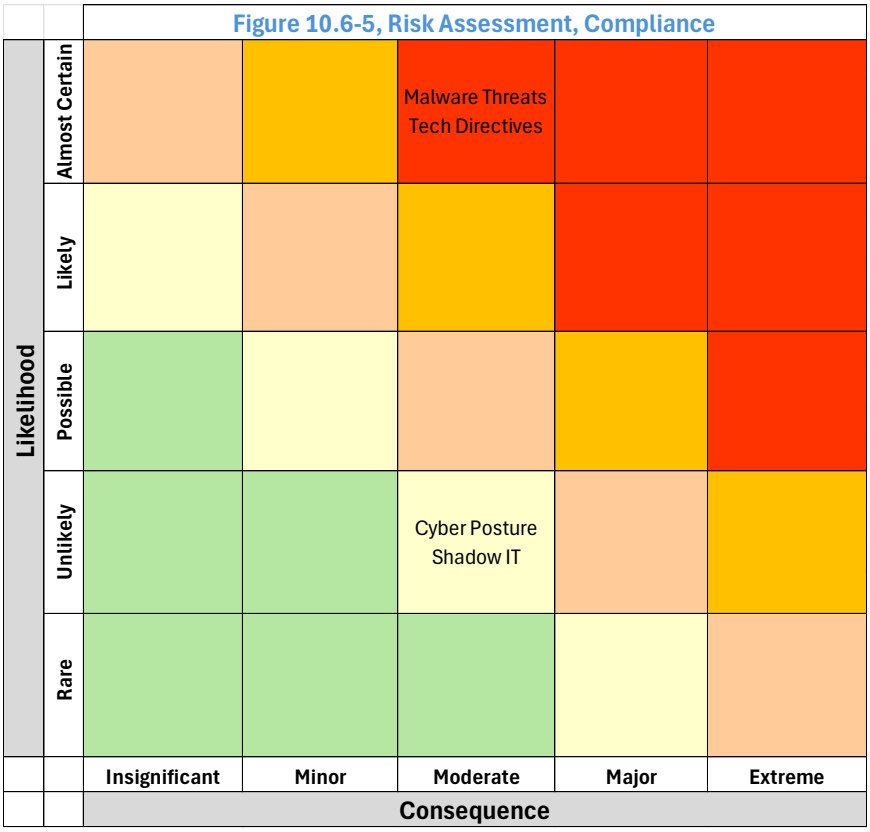


Figure 10.6-5, Risk Assessment, Compliance



11.0 ADDRESSING BARRIERS TO ACHIEVING OPTIMAL PERFORMANCE

Over the last four years, IT has shortened refresh rates to adopted industry best practice to refresh infrastructure and personal computing devices on a three-year cycle, although there remain a few outliers that have longer refresh cycles. Basic monitoring is performed for infrastructure devices, using established industry practices and to replace failing or failed devices. Infrastructure devices that reach their scheduled refresh rates are replaced. This scheduled refresh reduces problems with security patching, minimizes operating system upgrade issues, generally reduces overall expense costs, improves performance (taking advantage of latest hardware performance improvements), maintains security, and generally maintains a high level of asset reliability and performance. IT is providing higher priority to sustain activities to prevent degradation of IT asset performance caused by deferral of life cycle replacements that may occur as a result of constrained funding.

In order to avoid the temptation to defer refreshes of personal computing devices when a given fiscal year results in a reduction in expense, these devices have been moved to a 3-year lease program. IT is encountering lower overall costs in this area due to decreases in service calls, better device performance, and fewer issues with security patches. On the flip side, labor to swap out desktop devices is significant, and there is more frequent disruption to client use of these devices as replacements occur.

Applications are implemented and maintained to meet business needs. Capital investments for applications require a business case which requires the business needs and associated benefits to be identified. IT was partnering to build the practice of developing metrics to track applications' business benefits. The intent was to

use the business benefits as a means to measure how well an application asset is performing in meeting business needs. If the business benefits begin to trend lower, this would be an indication that the application is not meeting the business needs as effectively as it had been – the asset's performance is dropping. This would prompt an evaluation of why the asset's performance is dropping and how to restore business value. Does the asset need an upgrade, enhancement, or more substantial action such as replacement? Perhaps the business needs have changed to the extent the asset is no longer needed, prompting the asset to be retired. Unfortunately, reductions in staffing levels have reduced or eliminated this collaborative evaluation with our business customers. Re-stablishing the Office of the Chief Technology Officer may bring this effort back to the forefront.

IT created a set of health indicators to help monitor asset performance and to assist in moving assets toward sustainable optimal asset performance. These health indicators are described in Section 8. They are intended to monitor assets' ability to provide reliability, provide financial value, meet business needs, ensure security and reduce risks, and to deliver continuity of operations. The intent is to institutionalize these health indicators in the near future and to use these health indicators to drive decisions on future investments to deliver on acceptable levels of sustainable asset performance. Scarce funding has placed this initiative on hold. Re-stablishing the Office of the Chief Technology Officer may bring this effort back to the forefront.

The ability to hire appropriately skilled personnel into IT positions has developed into a serious problem. This manifests in two primary ways: 1) The unemloyent rate for IT positions in our area is very low, below 1.6%, leading to high demand and low supply, which results in commercial labor rates that cannot be matched by federal pay tables; and 2) the lack of support for full remote work at the agency is resulting in lower applicant levels, hiring offers turned down, and failed recruitments. IT is utilizing available hiring incentives to attract appropriate talent, as well as participating in OMB and DOE retention programs.

The outlook for IPR expense spending levels for IT could have a significant impact on the ability to execute capital spending on behalf of IT asset management programs, and the overall health of IT assets. Constrained expense spending in FY22 – FY25 could require further reductions in IT staffing, products, and services beyond reductions already experienced in the preceding years. This will likely lead to sub-optimal asset performance and unmet business demand. IT is working closely with the Office of the Chief Administrative Officer and lobbying the Finance Committee to secure adequate expense funding.

12.0 DEFINITIONS

Investment Classifications:

Compliance: Must be an executive order/directive requiring the specific investment must be made and that the project as proposed includes only the minimum required to comply with the directive. For example Cyber Security, Highway Relocations, BiOp

Replacements: In kind replacement of equipment and components. For example, wood poles, transformers, batteries, existing buildings, breakers, reactors, conductor.

Upgrades/Additions: Replacement of existing assets that provide addition capacity and/or capability. Examples include breakers, transformers, lines, etc. that after replacement have higher ratings to transfer power. Replacement of applications that provide new capability

Expansion – adding new assets to the system that did not exist before providing new capability. Examples include: new IT applications, new buildings, and new units at existing power generation sites, new line and substations.