S

# 2022 INFORMATION TECHNOLOGY STRATEGIC ASSET MANAGEMENT PLAN

*For "Information Technology (J-org)"*

The Information Technology Strategic Asset Management Plan (IT SAMP) 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 Bonneville Power Administration (BPA) staff to securely and reliably perform their business functions on a daily basis.

# Table of Contents

1.0 EXECUTIVE SUMMARY ..... 4
2.0 ACKNOWLEDGEMENTS ..... 5
2.1 Senior ownership ..... 5
2.2 Strategy Development Approach ..... 6
2.2.1 Key Contributors ..... 7
2.2.2 Key Activities ..... 7
3.0 STRATEGIC BUSINESS CONTEXT ..... 8
3.1 Alignment of SAMP with Agency Strategic Plan ..... 8
3.2 Scope ..... 8
3.3 Asset Description and Delivered Services ..... 9
3.4 Demand Forecast for Services ..... 11
3.5 Strategy Duration ..... 13
4.0 STAKEHOLDERS ..... 13
4.1 Asset Owner and Operators ..... 13
4.2 Stakeholders and Expectations ..... 14
*Table 4.2-1, Stakeholders* ..... 15
5.0 EXTERNAL AND INTERNAL INFLUENCES ..... 16
*Table 5.0-1, External and Internal Influences* ..... 17
5.1 SWOT Analysis ..... 19
6.0 ASSET MANAGEMENT CAPABILITIES AND SYSTEM ..... 19
6.1 Current Maturity level ..... 20
6.2 Long Term Objectives ..... 22
6.3 Current Strategies and Initiatives ..... 23
6.4 Resource Requirements ..... 25
7.0 ASSET CRITICALITY ..... 25
7.1 Criteria ..... 25
7.2 Usage of Criticality Model ..... 30
8.0 CURRENT STATE ..... 30
8.1 Historical Costs ..... 31
8.2 Asset Condition and Trends ..... 34
8.3 Asset Performance ..... 37

8.4 Performance and Practices Benchmarking ..... 41
9.0 RISK ASSESSMENT ..... 42
10.0 STRATEGY AND FUTURE STATE ..... 45
10.1 Future State Asset Performance ..... 47
10.2 Strategy ..... 47
10.2.1 Sustainment Strategy ..... 47
10.2.2 Growth (Expand) Strategy ..... 49
10.2.3 Strategy for Managing Technological Change and Resiliency ..... 49
10.3 Planned Future Investments/Spend Levels ..... 50
10.4 Implementation Risks ..... 53
10.5 Asset Conditions and Trends ..... 53
10.6 Performance and Risk Impact ..... 55
11.0 Addressing Barriers to Achieving Optimal Performance ..... 56
12.0 DEFINITIONS ..... 58

# 1.0 EXECUTIVE SUMMARY

**Benjamin L. Berry**
Executive Vice President
Information Technology and CIO

IT assets and funding are an extremely small percentage in terms of overall BPA levels. The services they provide have a profound impact on the effectiveness and efficiency of Bonneville's processes and people. The Information Technology Strategic Asset Management Plan (IT SAMP) is intended to ensure IT resources and investments are aligned with corporate vision and strategy to maximize business value and to achieve efficiencies where possible to reduce operating costs. However, not all investments have an immediate return or yield immediate benefits. The IT SAMP must also align investments to reduce risks to acceptable levels. One of the areas where planning and investments is needed to reduce risk is in delivering a viable disaster recovery service(s) for Bonneville Power Administration's Enterprise Business Systems (today BPA can meet its recovery time objectives for Mission Critical Systems).

The major outcomes of the IT SAMP are as follows:

- Evolving IT Infrastructure to meet emerging cyber security threats and providing reliable services while lowering operations and investment costs required to meet business needs, and
- Meeting strategic and evolving business needs by providing business solutions which deliver demonstrable positive net value and benefits to BPA and the Pacific Northwest.

The IT SAMP addresses significant external and internal influences facing Information Technology 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, IT Technological and Budgetary Challenges, and Strategic Partnerships.

In moving to the future state, IT will need 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 will need 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) will need to 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.

The IT SAMP also embraces both industry trends and the Office of Budget Management (OMB) guidance to consider cloud-based solutions. This trend will have a significant impact on the type of funding IT needs as cloud-based solutions require a higher proportion of expense funding instead of capital – capital is what IT has traditionally programmed for new business investments – which will result in IT capital and expense levels mixing in different ways.

Some significant changes to the IT landscape 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, with federal wages unabe to keep pace with commercial offerings.
  - 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.
- Increased cyber security threats 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.
- The recognition that maintenance contracts for IT goods and services continue to rise at a rate much higher than standard economic inflation, placing tremendous pressure on an annual IT budget that is composed of nearly 50% IT contracts.
- Reduced staffing levels as a result of constrined budgets in recent years must be restored to be able to maintain performance objectives for IT assets.

# 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 operations and maintenance (O&M).
- Become a strategic partner, advising and assisting business lines and BPA in leveraging technology to meet and achieve our objectives.

This IT Strategic Asset Management Plan represents a continuation in achieving these commitments. However, 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 additional cost efficiencies.

## 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 (SAMP) 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, Corporate lines of business, and the conducting of *"IT As A Customer Service Organization"* workshops with IT's business clients.
- Updates to the IT architecture are reflected in the various IT asset plans (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. This process is reaching the repeatable and standardized maturity level.

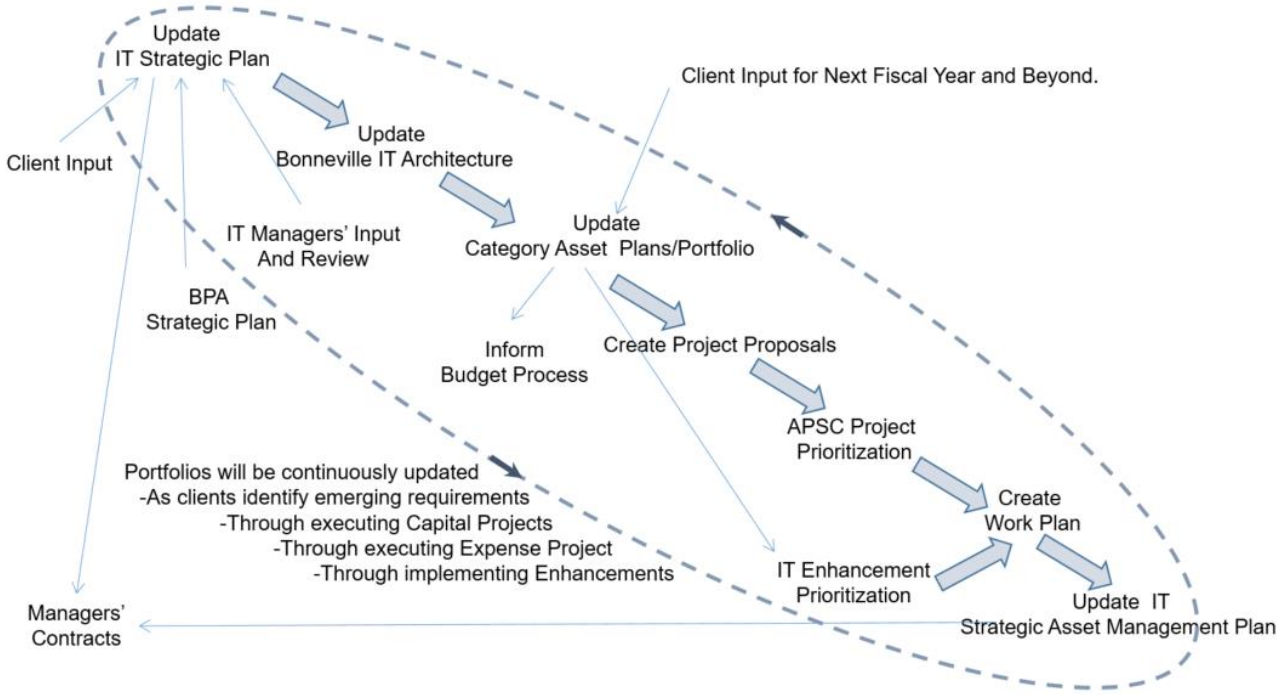



*Figure 2.2-1 Annual Asset Management Cycle*

### 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 Administrative Officer – who validates IT direction and goals for service delivery and ensures the IT SAMP sets the proper tone.
- Category Asset Managers – managers responsible for maintaining the Datacenter, Network, Office Automation, and Application asset plans (there are nine IT category asset managers).
- Information System Managers (ISOs) – 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 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.

Chief Information Officer – sets direction and goals for BPA Information Technology services and ensures business needs are prioritized and addressed.

### 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 both the BPA Information Technology Architecture (BITA) and 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.
  - Health indicators have been revised in FY2017 and 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 asset.
- Use IT asset plans to inform/update the IT SAMP.
- 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 FY2022 IT SAMP.

# 3.0 STRATEGIC BUSINESS CONTEXT

## 3.1 Alignment of SAMP with Agency Strategic Plan

Bonneville's mission is to create and deliver best value for its customers and constituents. It is committed to cost-based rates by setting rates as low as possible while maintaining consistency with sound business principles and ensuring full recovery of all of its costs. BPA's vision to be an engine of the Pacific Northwest's economic prosperity and environmental sustainability is provided through high reliability, low rates, responsible environmental stewardship and regional accountability.

The direction of BPA's Strategic Plan has set forth goals which will sustain and further BPA's mission and vision. To champion these goals, Information Technology has outlined objectives in the IT SAMP which are centered around 1) modernizing assets (BPA Strategic Goal #2) to help BPA maintain a competitive advantage in the marketplace and enable business units to deliver on public responsibilities; as well as 2) strengthen financial health (BPA Strategic Goal #1) through the management of lifecycle costs and asset value. The details of these objectives are described in section 6.

## 3.2 Scope

The Information Technology (IT) 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[1], and automated business solutions that enable BPA staff to securely and reliably perform their business functions on a daily basis. The IT SAMP does not cover information technology assets identified as Operational Technology (OT)[2].

[1] Servers, storage, laptops, workstations, thin clients, smart phones, etc.

[2] 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. Future replacement of the Dittmer Control Center (DCC) by a new Vancouver Control Center (VCC) will afford the opportunity to consolidate Portland and Vancouver data centers in which OT and IT will share facilities infrastructure while remaining independently funded.

## 3.3 Asset Description and Delivered Services

Information Technology BUD assets include: network/telecomm circuits, servers, storage devices, desktop systems, printers, copiers, faxes, phone systems, and software applications, including applications provided as Software-as-a-Service (SaaS). The automated solutions covered by this strategy include critical business systems and general business systems, as well as small single task-related applications specific to certain job roles. Critical business systems must operate and be available around the clock (24x7) 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 and manage their missions.

The IT Asset Portfolio is divided into four major sub-portfolios and each asset sub-portfolio has its own asset plan. We use this IT SAMP as guidance in preparation of those asset plans, which are used as components in creating our overall IT Asset Plan.

The Office Automation, Network, and Data Center sub-portfolios collectively form the information technology infrastructure that supports both users and systems. We will use infrastructure throughout this strategy to refer collectively to these three sub-portfolios. Table 3.3-1 describes each of the infrastructure sub-portfolios and the fourth sub-portfolio, applications.

*Table 3.3-1, Assets*

| Sub Portfolio | Assets | Activities | Benefits |
|---|---|---|---|
| Office Automation | Workstations, laptops, tablets, printers, productivity software, peripherals (scanners, portable hard drives, etc.), smartphones, cameras, monitors, projectors, and large format displays | ○ Refresh aging network printers and desktops/laptops and peripherals<br>○ Upgrading misc. productivity software<br>○ Adoption of new technologies<br>○ Obtaining/ensuring compliance with architectural standards and security controls | ○ Enables/supports user productivity by providing personal computing devices<br>○ Provides business and individual software solutions to improve productivity |
| Data Center | Servers (infrastructure servers, application servers, database, etc.) operating systems, database management systems, and management tools | ○ Refresh aging servers and storage<br>○ Migrating to new server operating systems<br>○ Adopting new technologies (virtual storage, server virtualization, cloud services, etc.)<br>○ Enhancement of data center (improving bandwidth, improving backup and recovery, server consolidation, etc.)<br>○ Obtaining/ensuring compliance with architectural standards and security controls | ○ Provides computational resources and storage to run BPA automated solutions<br>○ Provides storage for files<br>○ Provides email and calendaring services<br>○ Provides Cyber Security monitoring and mitigation |

| Sub Portfolio | Assets | Activities | Benefits |
|---|---|---|---|
| Network | Data, voice, and video networks. Includes fiber and cable plant, switches, routers, firewalls, web filters, Domain Name System Security Extensions (DNSSEC), Intrusion detection systems (IDS) and intrusion prevention systems (IPS), 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) | ○ Refresh aging network infrastructure (routers, switches, hubs, firewalls, cabling, etc.)<br>○ Enhancement of network infrastructure (remote access, wireless access, etc.)<br>○ Adoption of new technologies (tele-presence, messaging convergence, Internet Protocol version 6 (IPv6), etc.)<br>○ Obtaining/ensuring compliance with architectural standards<br>○ Enhancements/modifications to meet emerging security threats | ○ User access to network resources (internet email, files, print, business systems, phone, audio and video conferences)<br>○ Data center interconnections and intraconnections<br>○ Maintain security posture<br>○ Webcasts<br>○ Call center functionality for groups |
| 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:<br>• Real time or preschedule transmission or power scheduling<br>• Hydro operations<br>• Marketing (deal capture, day ahead trading)<br>• Short term forecasting, planning and loads<br>There are approximately 20 critical business systems.<br><br>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<br>○ Upgrades and/or enhancements (typically expense)<br>○ Software-as-a-Service (SaaS)<br>○ Applying system or security patches<br>○ Implementing new features to meet business needs<br>○ Correcting bugs or erroneous computing conditions<br>○ Implementing annual changes such as tax code changes<br>○ Retirement and/or disposition of systems<br>○ Maintaining systems in compliance with the enterprise architecture and security controls | ○ Provides automated business systems<br>○ Enables efficient and effective business processes and capabilities |

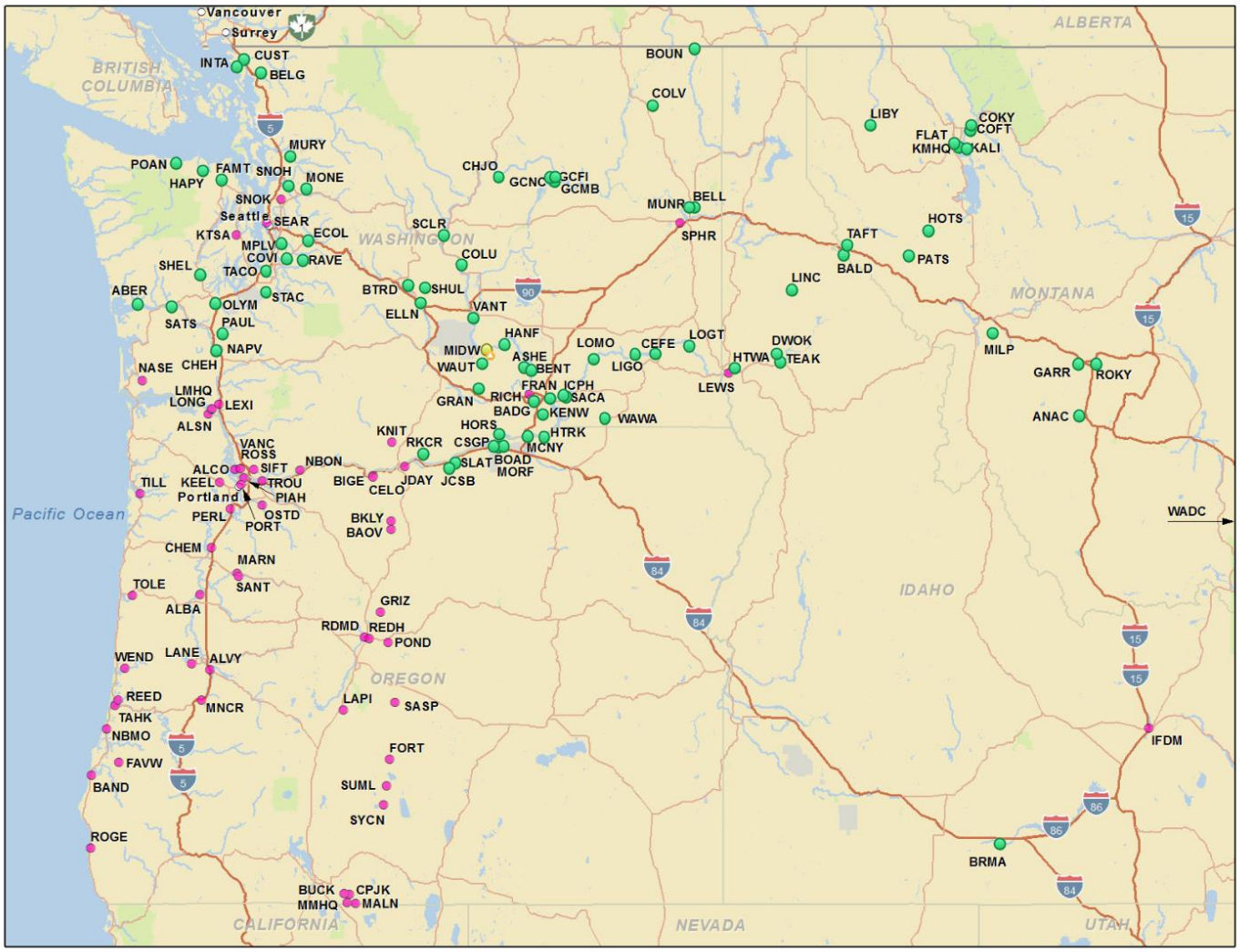



*Figure 3.3-2, Asset Locations*

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 Transmissions 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 of modernization and cost consciousness include components of 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.

Underlying these capabilities is the asset management objective that IT products and services result in more business value than the cost of maintaining them at an acceptable level of reliability, availability, and

serviceability. This idea can be encapsulated as follows: if we are going to implement and use an asset, we must maintain that asset. This implies prioritizing and planning the funding for various 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 capability, and performance monitoring.

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

- Grid Modernization – While great strides have been accomplished to move this effort forward, work remains to be done, and this is still the number one effort across BPA. IT will require completing enhancements or replacements of several IT systems such as Customer Billing, Agency Metering, Integration Services, Agency Enterprise Portal, etc. Preparation to participate effectively in the Energy Imbalance Market (EIM) is a major driver in this endeavor.

- 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 have gained even more importance in the shadow of the COVID-19 pandemic, driving increased performance requirements to support a much larger teleworkforce.

- Malware 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.

- Cloud Adoption – While the rate of cloud adoption has slowed somewhat from the initial hype cycle, the notion is still prevalent and likely to affect IT solutions into the future. The transition is likely to be 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 recently changed.

- Financial Modernization – On the heals of Grid Modernization, IT expects this effort to replace aging financial systems at the agency to become the next top enterprise effort. It will require prioritized funding over a multi-year period.

- Enterprise Asset Management Maturity (EAMM) program – In November 2021, the Enterprise Architecture Governance Committee (EAGC) approved a mulit-year collaboration between business units, the Business Transformation Office (BTO), and Information technology (IT) to mature asset management capabilities across BPA. The program objectives are to plan for enterprise asset management maturity, introduce new business planning and data management requirements, steadily reduce technical debt, and ensure all teams working on projects related to asset management maturity remain aligned, supported, and informed. This workload is in the early stages of definition, but is expected to organize a consistent approach to asset management, including consolidation of asset management automated systems, across the agency.

- 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 Information Technology Strategic Asset Management Plan covers a five-year window with an annual review, and a published update every two years, unless there is a significant change in the strategy at the annual review. Drivers that may cause changes to the SAMP include:

- Rapid pace of change in IT
  - 3 years is a hardware generation
  - 3-4 years is a software generation
  - Rapid adoption by industry of new disruptive technology
- Evolving cyber security threats that require immediate counter measures
- New and disruptive federal guidance (i.e., Cloud Smart, DOE Order 200.1.a, DCOI, etc.)
- Completion/updates to BPA business strategies/roadmaps

## 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[3]. 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 projects.

All assets and services are put in place in order to meet the business needs of the Information Owners[4] (IOs). The assets are maintained and operated by Information System Owners (ISOs). ISOs are IT managers or their delegates. ISOs work with the IOs to ensure IT assets, services and automated systems:

[3] 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. The CIO and Supply Chain are working 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.

[4] 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's managers (i.e., managers in Power, Transmission, Corporate, EF&W, etc.).

- 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, 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. These areas of mutual dependencies are summarized by:

- IT supports moves, additions, and deletions of personnel.
- Facilities provides and maintains cable plants (physical wire/fiber used by IT networks).
- Facilities maintains existing infrastructure and provides new infrastructure to house, operate, and secure IT resources.
- IT provides new infrastructure (ensuring IT resources are positioned to meet building(s) computational requirements).
- Facilities maintains tiered data center(s) at appropriate availability and PUE ratings.
- IT provides storage and retrieval capabilities for physical security data related to cameras.
- IT provides network connectivity for physical security assets.
- Physical security provides live monitoring and reporting, and card-lock capabilities to IT data cenetrs and equipment 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. Providing personal information technology services/commodities has evolved from "Give me what you have and I'll make it work" to "Give me what I want that already works". The way in which IT has been traditionally funded has led to this environment of entitlement where consumers believe they have already paid for IT services and therefore can obtain whatever they want without consideration of cost. This results in 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 |
| | Assets meet reliability objectives by being refreshed based on published refresh rates, and design meets availability requirments | IT Asset Plan Health Indicators | Asset Health Indicators |
| ***Chief Information Security Officer*** | IOs/ISOs 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 | BITA, 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 Plan Health Indicators | 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<br><br>SLA targets/metrics |
| | Assets are enhanced to meet evolving and emerging business needs | Asset Plan | Asset Health Indicators |
| | New systems/automated solutions are delivered to meet evolving and emerging business needs | PMO Work Plan<br><br>PMO Monthly Status Report | Project Health Indicators |

| Stakeholders | Expectations | Current Data Sources | Measures |
|---|---|---|---|
| ***IT Services Consumers (personal computing devices end users, etc.)*** | Modern, reliable desktop and mobile personal computing devices | 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, etc. | Submissions to CPIC | Various data calls |
| | 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, salmonrecovery.gov, 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 budget constraints in FY19-FY21 were difficult to overcome, however cooperaton among the organizations within the Chief Adminstrator's Office and service reductions enabled IT to meet the highest priority demands. Successful negotiation of increased spending levels for IT beginning with the FY2022 budget cycle enables us to barely maintain operations at the current level, but still leaves scant room for additional system implementations to meet emerging business needs and new regulatory requirements. Staffing reductions have resulted in service reductions and lower reliability and availability of products and services, leading to more frequent system outages. The end result is that under funding IT is resulting in shrinking capabilities. The road to recovery must continue.

*Table 5.0-1, External and Internal Influences*

| External Influences | Affects and Actions |
|---|---|
| OMB Cloud Smart Guidance<br>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). |
| OMB Data Center Optimization Initiative (DCOI)/ OMB M-16-19 and M-19-19<br>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, 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 facitlity to accommodate the HQ data center. |
| Federal Information Technology Acquisition Reform Act (FITARA) /DOE Order 200.1A<br>(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<br>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. This has the potential to wreck havoc, especially for legacy software systems. |
| Rate of Change in IT<br>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)<br>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**. |
| COVID-19 Pandemic<br>A sustained time period in maximum telework status creates some unique issues for IT service delivery by limiting access to physical assets, and lengthening the time for vendors to deliver products. | The impact to BPA is a shift and lengthening of schedule to accomplish lifecycle replacement activities for office automation, data center, and network sub-portfolios. This potentially affects the entire PMO portfolio of IT projects, and may shift funding to subsequent fiscal years. Global silicon shortages and supply chain delivery interruptions magnify the problem. Earlier planning, design, and procurement will likely be required. |

| Internal Influences | Affects and Actions |
|---|---|
| Maintaining an IT Investment Program<br>IT capital investments have been delivering new business systems into production at the rate of about six new systems a year between FY2008-FY2019. That rate has dropped to 1-2 in FY2022. | 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. **IT has not been fully funded to maintain the net new O&M from these new systems**. This has created a backlog in enhancements to existing systems and new systems (insufficient expense available to move a project from initiate to execute, the phase where capital can be used). **Maintaining existing systems and commitment to Grid Mod/EIM consume nearly the entire IT project budget**. |
| Evolving Business Unit Roadmaps<br>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) will work 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<br>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 hardware refreshes, resulting in aging hardware with lower reliability; and software upgrades, 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)<br>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.<br>**The IT Asset Manager is now requiring that system designs include DR as part of new design**; 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<br>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**. |
| Business Value<br>Prioritizing development and deployment of new assets (business solutions) based on net value. Identifying and tracking business value. | Discretionary investments should be made based on the ability of the solution to produce enough business value to recover the investment and annual maintenance and enhancement costs. IT is slowly working with IOs to institute robust mechanisms and processes to track and report on business value. **When a system's business value drops below the annual cost to operate, a decision needs to be made to either restore value (e.g., enhancement or upgrade), replace, or retire**. |
| IT Workforce<br>BPA expects to see 25% of its IT federal workers retire in 3 years and 50% in 8 years. | 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) to attract top talent. 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<br>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*** | ***Weaknesses*** |
| • Technical acumen.<br>• Ability to use automated discovery for some asset inventories.<br>• Robust IT PMO and SLC practices.<br>• Solid change management system to enable asset maintenance with least impact. | • Transparency of IT costs.<br>• Ability to say no to resource requests.<br>• Longer term planning of asset replacements/upgrades.<br>• Connection of enterprise architecture to technical architecture.<br>• Separation of IT & OT business functions.<br>• Clients not directly involved in IT funding. |
| ***Opportunities*** | ***Threats*** |
| • Availability of IAM certification training.<br>• Consolidation of enterprise asset management systems.<br>• Adoption of ITIL framework includes a CMDB to link assets to services.<br>• Maturing of IT Service Catalogue | • Availability of funding for asset life cycle management.<br>• Rising rates of hardware and software maintenance contracts.<br>• Rising rate of technology change shortening asset life expectancy.<br>• Increasing security threats.<br>• Scarcity and rising cost of IT labor. |

# 6.0 ASSET MANAGEMENT CAPABILITIES AND SYSTEM

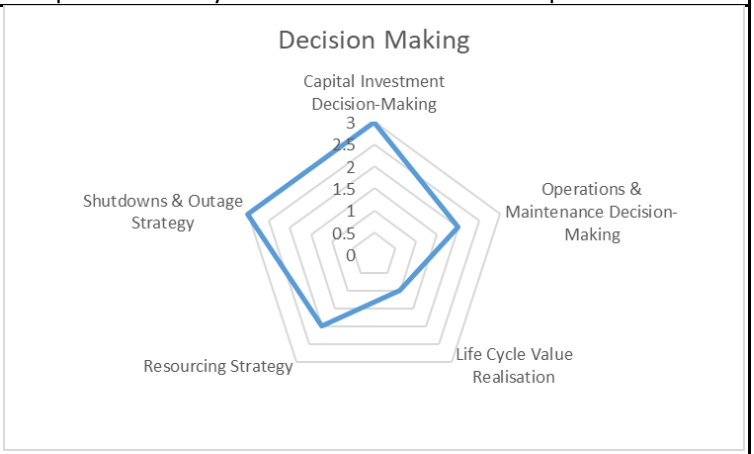
Averaging the maturity level of each of the six subjects groups, IT lands at a rating of 1.6, which is between Developing and Aware, and is likely a fair assessment. In summary, IT is fairly good at keeping assets operational. It is marginal at

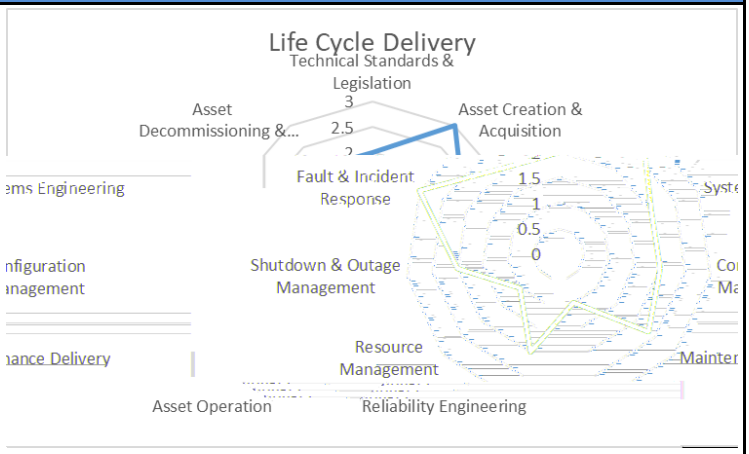
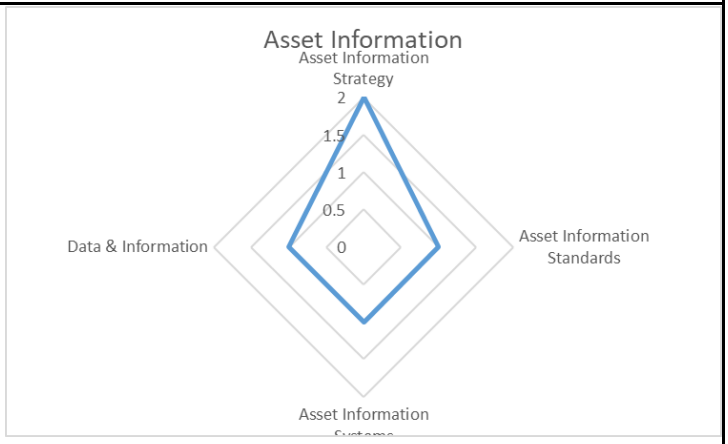
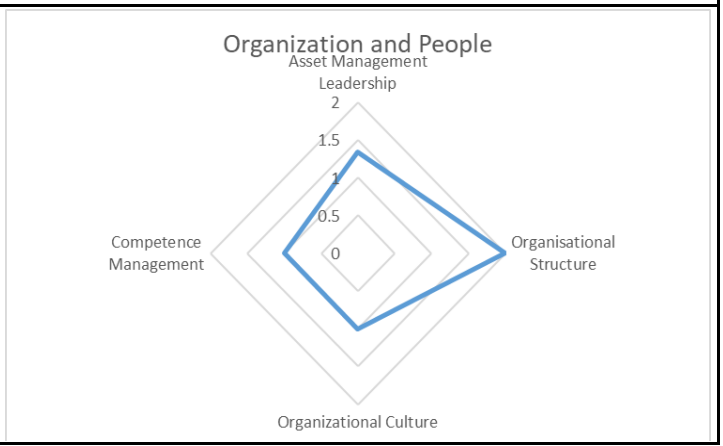
resource management. This is primarily due to two factors: IT uptime has been a major goal and metric for many years, and budgets are generally top-down and maintenance contract costs are controlled by limited vendor competition.

## 6.1 Current Maturity level

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 1.5. **Strengths:** The IT organization understands the specific maintenance activities required to keep its assets in an operational condition. **Weaknesses**: Asset plans exist either as as records in the Project Performance Management System or Excel spreadsheets 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 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 2.<br>**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.<br>  <br>**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 1.2.<br>**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.<br>  <br>**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 1.3.<br>**Strengths:** Procurement and supply chain processes are in place.<br>**Weaknesses:** Organization and leadership strategy around asset management is lacking. Asset management is not a key factor in the IT culture.<br>  |

| Subject Area | Maturity Level | |
|---|---|---|
| Risk & Review | Risk & Review in the IT organization is at a maturity level 1.4.<br>**Strengths:** Resources are available for peer review across portfolios and sub-programs.<br>**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 (IAM) into IT's cultural change from providing technology to being a service-oriented business partner to the agency. Since IT does not have a large pool of resources to assign to this, the progress is expected to be mild but steady.

IT is partnering with the Business Transformation Office (BTO), business lines, and the BPA Asset Manager to stand up an Enterprise Asset Management Maturity (EAMM) program. The concept was approved in November 2021. Charter development is underway and the program is on track to deliver the first draft of a sequenced plan to mature asset management capabilities (rolling 5-year window) by the end of FY2022. The EAMM will converge strategic priorities across the enterprise into a shared target state, plan/sequence initiatives from business and IT into a common roadmap, and enable the funding and implementation of more sustainable and architecturally acceptable solutions.

Table 6.2-1 outlines the underlying objectives to meet the overall goal, distributed across the IAM subject areas. To match BPA's current top priority regarding cost effectiveness, the priorities of the objectives are centered around finance and budget, and sequencing considers dependencies between objectives and the potential to address some of them in parallel.

*Table 6.2-1, Long Term Objectives*

| Subject Area | Maturity Level | Timeframe | Sequence | Priority |
|---|---|---|---|---|
| Strategy & Planning | **Objective:** Sub-program asset plans will be centrally managed in a common enterprise application/repository using consistent style and content. | Q4 FY22 | 3 | 3 |
| Decision Making | **Objective:** Decision making will include broader business line participation and will take out-year O&M activities into consideration. | Q4 FY23 | 3 | 3 |
| Life Cycle Delivery | **Objective:** Solution development and operational maintenance activities will not contend for the same human resources. The timing aligns with staffing plan requests. | Q3 FY25 | 2 | 2 |
| Asset Information | **Objective:** Sub-program asset information will be centrally managed in a common role-based enterprise application/repository that is easy and intuitive to use and maintain, using consistent style and content. | Q4 FY23 | 5 | 4 |
| Organization & People | **Objective:** Asset Management will be the primary factor in all IT roadmaps and technology and budgeting development. This aligns closely with participation in an Enterprise Asset Management Maturity (EAMM) program. | Q1 FY24 | 1 | 5 |
| Risk & Review | **Objective:** Risk assessment will be included in budget planning for asset management life cycle activities, more closely linked to IT roadmaps. | Q3 FY22 | 2 | 2 |

## 6.3 Current Strategies and Initiatives

IT assets can be broadly grouped into two categories. The first is Infrastructure assets (Office Automation, Data center, and Network sub-portfolios) and the second is automated business solutions in the Application sub-portfolio. Each of these categories has different decision-making criteria and levels of maturity. Decision-making and life cycle delivery for Infrastructure and Applications follow the Agency Prioritization Steering Committee (APSC) process and solutions are delivered into production using the published BPA System Life Cycle (SLC). Table 6.3-1 describes the current strategies and initiatives under way to support IT's asset management objectives, distributed over the IAM subject areas.

*Table 6.3-1, Strategies and Initiatives*

| Subject Area | Key Initiatives |
|---|---|
| Strategy & Planning | **Strategy:** Consolidate/rationalize asset management systems and mature business processes, data management, and technical support to mature enterprise asset management capability.<br>**Initiative:** The Enterprise Architecture Governance Committee (EAGC) approved a new program, the Enterprise Asset Management Maturity (EAMM) Program. Key maturity initiatives will be to rationalize the IT asset management system portfolio (consolidate tools), establish an agency asset register, establish unique asset identifiers, implement infrastructure needed to meet asset segment architecture objectives. The program will work with the Asset Management Council (AMC) to refine the next target end-state (architectural plateau), consolidate all asset management related initiatives (in-flight or planned), and produce a 5-year sequenced plan by the end of FY2022.<br>**Strategy:** Standardize IT asset plan development and plan management.<br>**Initiative:** Refine the IT asset plan processes and select a target solution for centralized storage and management of the plans by the end of FY2023. |
| Decision Making | **Strategy:** Encourage and partner with business leaders to jointly define long-term automation needs and the funding requirements to maintain them.<br>**Initiative:** Pilot a new approach for business planning and prioritization of technology needs through the Enterprise Asset Management Maturity (EAMM) program. |
| Lifecycle Delivery | **Strategy:** Separate the solution development staff from the operational maintenance staff.<br>**Initiative:** Leverage the FY2021 Workforce Strategy to obtain enough appropriate skillsets that enable separation of development and operations work by the end of FY2025. Set aside managed services contract budget to provide development skillsets where needed and within budget constraints starting in FY2019 and continuing through FY2024. |
| Asset Information | **Strategy:** Collaborate among the sub-program category managers to consolidate into a standardized asset information repository.<br>**Initiative:** Implement the common Configuration Management Database (CMDB) that is a component of IT Service Management (ITSM), a maturity framework for improving the delivery of IT services, by Q2 of FY2023. Migrate all IT asset information into the CMDB by end of Q4 FY23. |
| Organization & People | **Strategy:** Prepare ahead of time for attrition of current asset management staff in the OCIO.<br>**Initiative:** Develop an IT asset management succession plan by the end of FY2022. |
| Risk & Review | **Strategy:** Inform budget planning with health and end-of-life information for IT assets.<br>**Initiative:** Include health indicators in portfolio asset plans by end of FY2022.<br>**Initiative:** Re-institute quarterly review of IT portfolio asset plans by the IT Asset Manager by Q3 of FY22. The reviews will validate risk identification and management by ensuring that asset plans include asset health indicators and activities to mitigate risks to acceptable levels. This will tie into IT Roadmaps. |

### 6.4 Resource Requirements

There are two primary functions within IT asset management that require resource identification and specific funding: maintaining the assets we currently own, and adding assets to the portfolio to meet emerging business demands. IT asset management itself, and the initiatives identified to improve that practice, are considered to be emerging demands. The growing cost of O & M expense tails for exsiting assets and new assets going into production in the last few years, and IT budget constraints between FY18 anf FY23, have severely reduced IT's capacity to add new automated solutions in FY22 and beyond. While some budget capacity was restored in FY22, that still mostly addresses existing assets and compliance requirements.

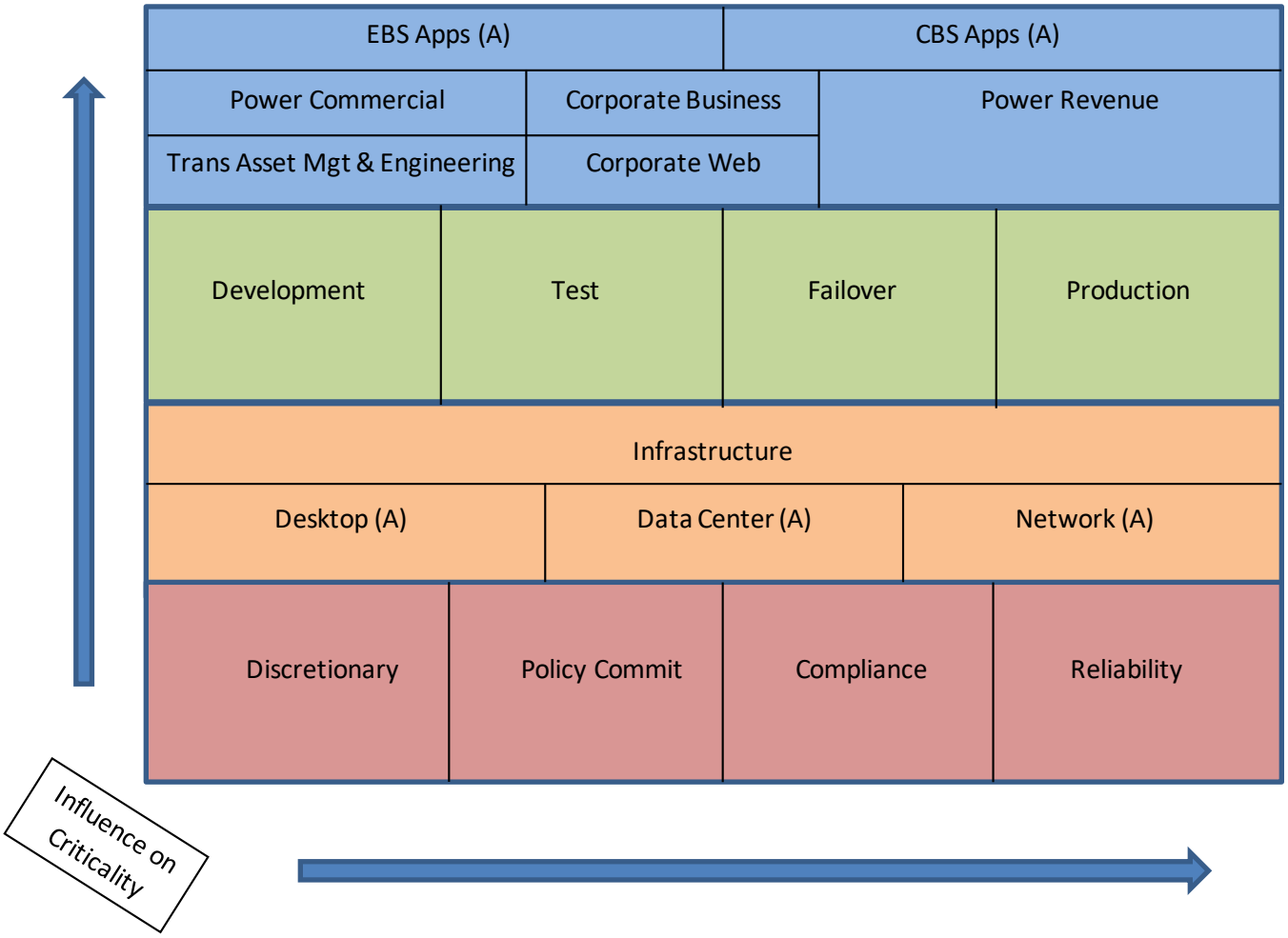
In order to successfully address the IT asset management maturity initiatives described above, we will have to successfully lobby for additional funding in IT. This will take the form of some additional staffing to relieve operations staff from project work, possible support from managed services contracts, additional staff in the OCIO for oversight and management of asset management programs, and some IT PMO formal projects for process improvement and automation of enterprise capabilities.

## 7.0 ASSET CRITICALITY

### 7.1 Criteria

The diagram below depicts the layers of criteria in order of precedence from least importance in the lower left, to most importance in the upper right. The items with (A) behind them are physical assets such as applications, servers, and network switches. The green bar presents the various environments in which IT assets are deployed, and the red bar describes the type of operational area, or commitment, supported by the asset.

IT assets are classified into two major areas: Enterprise Business Systems (EBS), and Critical Business Systems (CBS). EBS systems are those that support general operations for conducting agency business, such as Human Capital Management, Fleet and Facilities inventory, etc. CBS assets are those that provide or directly support revenue generation for the agency, such as trading floor applications, power scheduling, and such. CBS systems take precedence over EBS systems.




Within each of these two major classifications, the IT applications, computation, storage, network devices, and personal computing devices that comprise the systems are distributed across four distinct environments:

- Development (lowest criticality)
- Test
- Failover
- Production (highest criticality)

The life cycle of each system progresses from development, through test, and into failover and production. Production takes precedence over Failover, Test and Development. The CBS production environment is maintained at 99.9% availability with a requirement to fully failover to an alternate data center within twenty minutes of the loss of the primary computing data center. The EBS production environment is operated to meet 98.5% availability, with failover capability currently being matured.

The operational areas are used to further determine criticality for deciding asset management activities:

- Reliability – the effect on expected uptime.
- Compliance – the effect on meeting regulatory obligations.
- Policy Commit – the effect on meeting agreed-to obligations.
- Discretionary – Not strictly required, but very helpful none the less.

Table 7.1-1 provides some examples of system criticality information contained within IT's Application Inventory Management (AIM) system, currently the asset repository for all IT systems on the BUD network.

*Table 7.1-1 Examples of IT System Classification*

| 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. | |
| 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. |

| Business Function | Systems | Classification & Ops Area | Contribution of Service | Impact of Failure/ Business Continuity |
|---|---|---|---|---|
| | 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:<br>• Inability to record project and work order status for financial reporting, maintenance tracking.<br>• Inability to procure and distribute supplies and materials for necessary maintenance and construction activities<br>• 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.<br>• 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. |
| | 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:<br>• Inability to receive incoming revenue.<br>• Inability to make vendor and contract payments, thus incurring interest penalties and potentially losing lines of credits or preferred status.<br>• Unable to close month-end/year-end.<br>• Unable to account for assets and/or liabilities.<br>• 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 diagram 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 in the table 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 table 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.

As this approach to criticality and action determination becomes more mature, IT may design and adopt a scoring system to overlay the diagram to more clearly resolve potential conflicts.

## 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.[5]

[5] 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.

## 8.1 Historical Costs

IT capital investments have been delivering new business systems into production at the rate of about six new systems per year between FY2008-FY2019, reducing to three in FY20 and two in FY21. These new systems expand IT's assets resulting, on average, net new operation and maintenance (O&M) costs of 12.4% of the investment cost, due primarily to new software maintenance contracts and new support labor costs . At the same time, the IT expense increases have not kept up with the rate of inflation for maintenance contracts and the cost of labor, and the net new O&M costs from these systems. In fact, the budget levels for IT have dropped from approximately $98M Expense and $25M Capital in FY19 to $83M Expense and $21M Capital in FY20. Although the IT expense budget was restored to $101M in FY21, that almost covers the requirements just for maintenance of what we already own plus compliance requirements, particularly around cyber security. This practice and has resulted in:

- Increased backlog of business-requested enhancements to existing business systems.
- Increased backlog of business capital investments (Note: insufficient expense funds will prevent a capital project from entering and completing initiation and planning; capital cannot be used until an IT project reaches execution and it typically takes 20% of the investment cost in expense to carry a project from proposal to execution).
- Reduced FY22 projects to Grid Mod and Core Sustain efforts only.
- Caused IT to seek specific business line funding, as well as other sources, to accept projects for new systems.

Table 8.1-1 shows the historical spend based on project actuals and projections as reported through the IT Program Management Office. Note that while this table includes all capital expenditures in IT, it does not include the total IT expense budget. Not all IT expense is dedicated to asset life cycle.

*Table 8.1-1 Historical Spend*

| Program | Historical Spend (in thousands) With Current Rate Case | | | | | |
|---|---|---|---|---|---|---|
| Capital Expand (CapEx) | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 Projected |
| Apps | $4,300 | $5,810 | $2,110 | $8,700 | $5,020 | $4,400 |
| Data Center | $2,550 | $0,880 | | $2,800 | $0,480 | |
| Network | | | | | | |
| **Total Capital Expand** | $6,850 | $6,690 | $2,110 | $11,500 | $5,500 | $4,400 |
| Capital Sustain | | | | | | |
| Apps | $0,050 | $2,910 | $2,190 | $1,300 | $9,718 | $6,528 |
| Data Center | $1,000 | $1,544 | $1,748 | $5,326 | $7,000 | $3,500 |
| Network | $2,800 | $3,100 | $3,700 | $2,600 | $2,600 | $5,500 |
| **Total Capital Sustain** | $3,750 | $7,554 | $7,638 | $9,226 | $19,318 | $15,528 |
| **Total Capital** | $10,600 | $14,244 | $9,748 | $20,726 | $24,818 | $19,928 |
| Expense (OpEx) | | | | | | |
| Exp to execute Cap | $3,500 | $5,700 | $11,530 | $6,436 | $6,740 | $5,000 |
| **Total Expense** | $3,500 | $5,700 | $11,530 | $6,436 | $6,740 | $5,000 |

Figure 8.1-2 depicts the asset spending for the last five years. The actual numbers are accurate enough to show the trend although not exact since IT has not historically tracked the spend in this way.

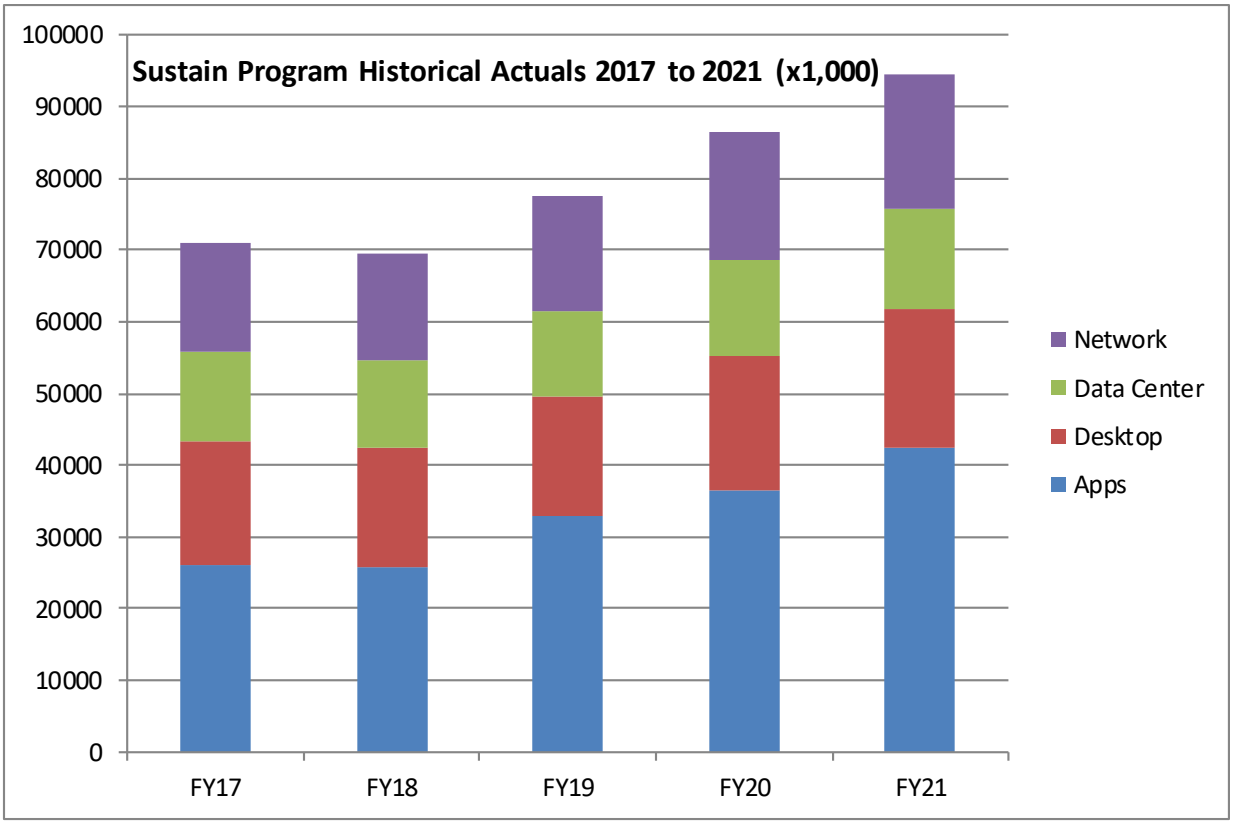



*Figure 8.1-2 Sustain Program Historical Spend*

The Business Transformation Office (BTO) is charged with the execution of Grid Modernization initiatives (Grid Mod). To achieve these efforts requires a combination of ehancements to existing systems, implementation of new automated systems (both on premise and cloud-based), and extensive integration of these systems. All of this growth in automated solutions has put pressure on existing assets and resources, while containment of growing IT costs is also an important objective.

To control the growth in labor from new systems, IT has had to embrace and leverage automation to reduce the number of Full Time Equivalents (FTEs), both contractor and federal, even as new systems are delivered into production. While the number of business systems continued to increase, IT has experienced an aging federal workforce that may see 25% of the federal IT workforce retire in the 5 next years and 50% in the next 10 years. Currently the IT workforce consists of approximately 44% federal and 56% contractors and on-site managed services. IT will need to continue to develop its workforce strategy with emphasis on attracting and retaining

adaptive IT workers capable of adopting emerging skills, such as cloud development, in a very competitive market. The recent Workforce Study performed by Human Capital Management set the appropriate personnel levels at 211 federal, with a projected 170 contractors plus on-site managed services. IT is targeting to reach these levels over the next few years, and with the added complication that most CFTE positions must transition to BFTE positions.

In FY19 spending priorities had to be changed within IT 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. IT also experienced a large shift from capital to expense for the Asset suite 9 upgrade. This software upgrade was originally programmed as capital, but the solution was determined to be expense.

IT capital spending was expected to level off and perhaps drop in the out-years due to an increasing adoption of Software as a Service (SaaS). SaaS solutions, as well as other cloud-based solutions – Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) – were predicted to be completely funded by expense. However, recent changes in government guidelines allow for capital spending for some cloud-based activities, and cloud vendors are offering solutions with contractual components that allow for a capital determination (e.g. transfer of cloud software and licenses to on premise). Under current agency conditions, where there is more capital headroom than expense, this has enabled implementation of more new IT projects, particularly in the Grid Mod/EIM portfolio. However, expense required to execute on capital, and the expense increase in annual O&M must also be taken into consideration.

## 8.2 Asset Condition and Trends

Up until 2019, new system requests were generally afforded higher priority over core-sustain efforts in order to meet emerging business line requirements for automation to improve their efficiency and effectiveness. After several years of this type of operating, and in conjunction with projected shrinking of available funding, IT realized that services had begun to deteriorate due to inadequate staff availability for operational support, and the growing backlog of needed age-based asset updates. Prime application examples of this are Asset Suite, Transmission Circuit Information System, EE Tracking and Reporting, Customer Portal, SharePoint, among others. Desktop computing equipment was reaching eight years of age due to several deferrals of equipment refreshes, including the desktop and server operating systems. Outages began to increase in basic systems such as Exchange and cell phone services. The most dire of these situations are currently being mitigated through updates or replacements, but the backlog is still significant and must be continuously addressed. In FY19 and forward, IT placed higher premium on core-sustain efforts for systems already in place, and that practice is continuing through FY24/25. Interestngly enough, DOE Enterprise Architecture has adopted standards requiring products to ramain within one version behind current, which has been a stretch target for BPA for some time.

Figure 8.2-1 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.

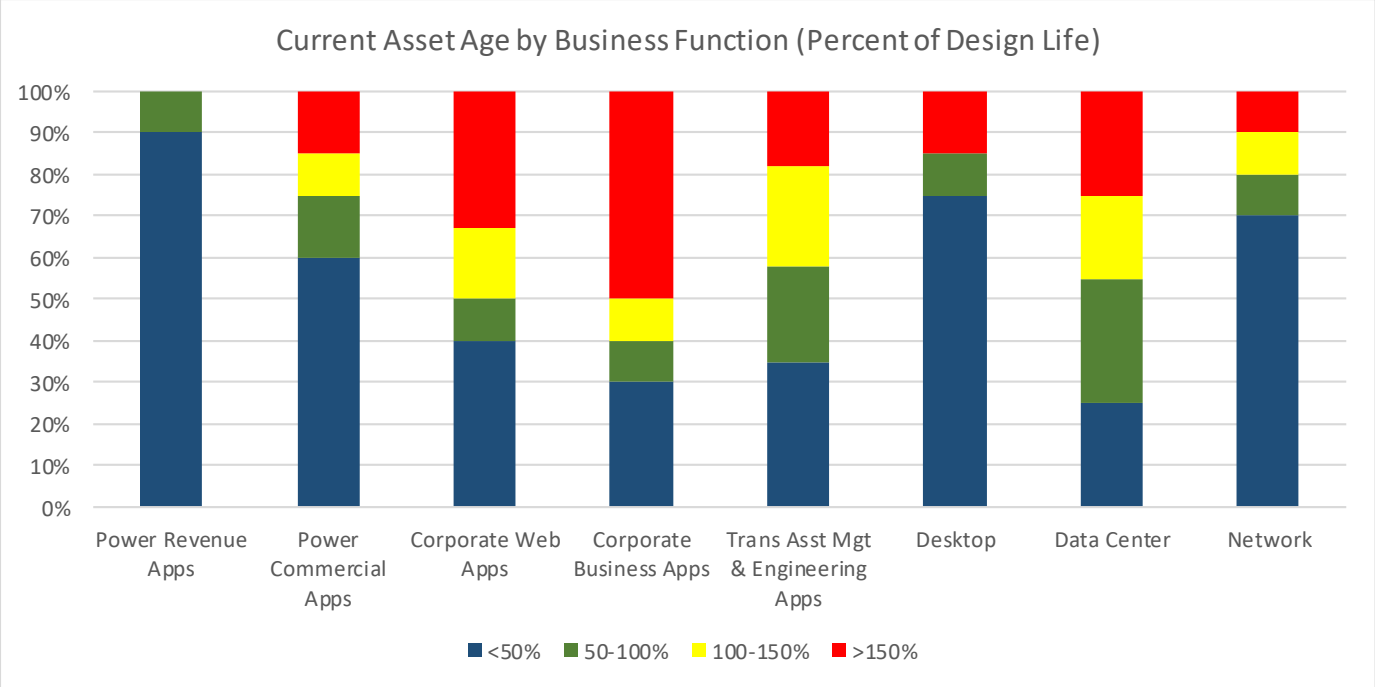



*Figure 8.2-1 Current Asset Age by Business Function*

Power Revenue Apps are in top condition (mostly blue) due to major systems being put into production within the last couple of years (TMS ➔ ETRM, for example), and the last two years have been dedicated to upgrades for preparation to enter the Energy Imbalance Market (EIM), increasing data analytics capabilities, and Mission Critical Integration replacement.

Power Commercial Apps is partially red due to the EE Interim Solution being "interim" for several years. EE Tracking & Reporting is nearly complete to replace it. Residential Purchase and Sales Agreements was recently updated to correct security vulnerabilities, returning it to blue status.

Corporate Web Apps is in dire straights for the Customer Portal and SharePoint systems. They are running on old versions of SharePoint, highly customized, and aging infrastructure. Fortunately, there is a project in progress to correct these back to blue within the next year.

Corporate Business Apps completed a major upgrade that moved its oldest systems (Asset Suite) back to top condition. There is also an upgrade for the systems in the yellow, BPFAS and Financial Planning, moving to cloud delivery. Customer Billing and Agency Metering are currently finishing up with replacement driven by Grid Modernization. Financial Modernization is an additional concet that is expected to deveop within the next year or two.

Transmission Asset Management and Engineering Apps will be bolstered by the Transmission Circuit Information System that is currently in progress, and the Aircraft Services Scheduling underwent emergency replacement due to a recent end-of-life announcement from the vendor. Cascade does not currently have an upgrade in progress, but will soon reach an age of concern, and so is yellow.

The Desktop function has an implementation of Cherwell Management Suite in progress that is due to come on-line this year to replace the Customer Relationship Management ticketing system currently in use. This is a major step toward transition of IT to Service Management.

In the Data Center, Exchange Email is in top condition, havig recently transitioned to cloud-based delivery per mandate from DOE. The primary issue for Data Center is the continued presence of Windows Server 2008. It is being updated, but the progress is slow since application testing resources are mostly scarce.

Network does not depend on many applications, but the CISCO management tools, and monitoring tools are largely up to date.

Figure 8.2-2 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.

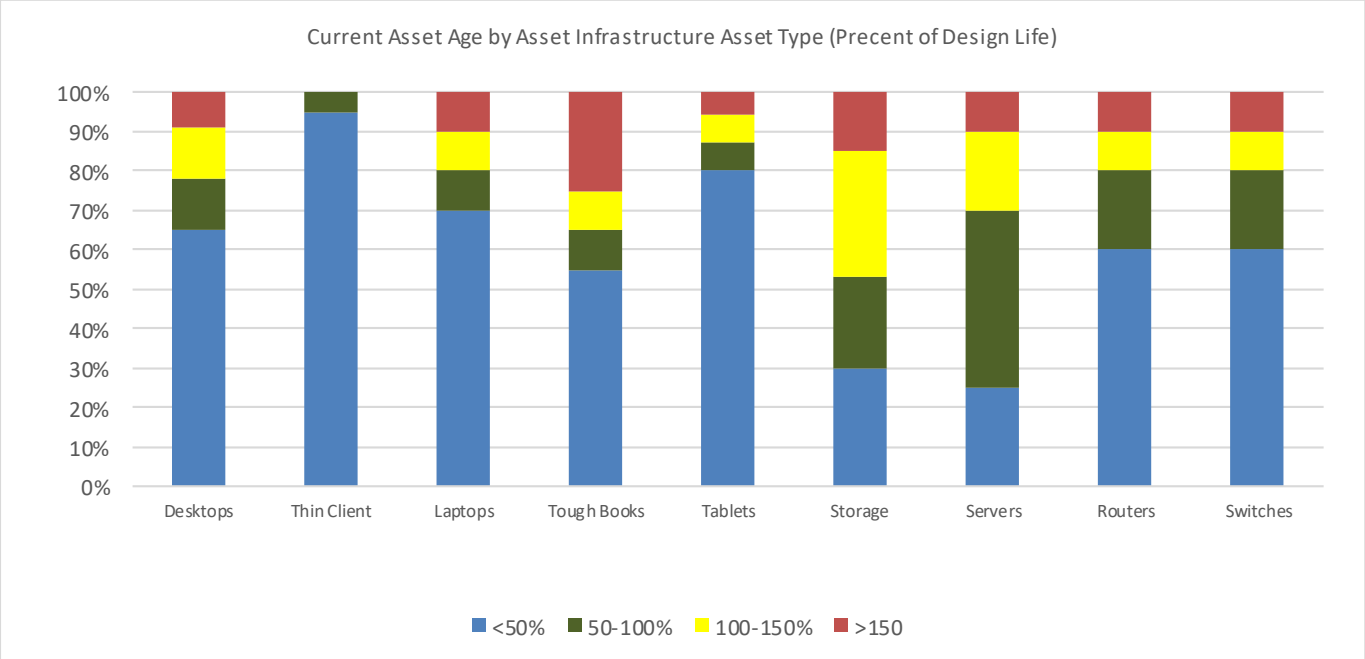



*Figure 8.2-2 Current Asset Age by Asset Type*

Desktop equipment is in much better shape now than in the last several years due to wholesale upgrades based on equipment leases. Lease replacements will commence in FY22, to include operating system upgrades. Network equipment has been on an annual percentage upgrade path for some years, and the pattern there is expected. Servers and storage have changied 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 FY2025.

## 8.3 Asset Performance

Until recently, 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. The last desktop refresh effort ushered in a new technical measure: startup time near 60 seconds.

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. A first run at establishing these health indicators was completed in FY2017, however reductions in staffing have prevented their adoption. The set of five metrics to measure the health of IT assets 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.

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 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.<br><br>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.<br><br>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:<br>• A enhancement or project is flight to drive the annual benefits to be greater than annual cost of operation.<br>• 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:<br>• An enhancement or project is flight to drive the annual benefits to be greater than annual cost of operations.<br>• 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.<br><br>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 held a workshop two years ago with a large cross-section of IT service providers and their customers entitled IT As a Customer Service Organization. The theme of the workshop was to engender a change in IT delivery from one of providing technology to providing services. Included in that was identifying what is important to the IT customers, and metrics and measures that are important to them. Due to budget contraints, the ITSM program is currently on hold.

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 enough to publish with any sense of accuracy. 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.

## 8.4 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

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

| Impact Level | SAFETY | RELIABILITY | FINANCIAL | ENVIRONMENTAL | COMPLIANCE |
|---|---|---|---|---|---|
| | 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 |
| Impact: 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 I 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 |

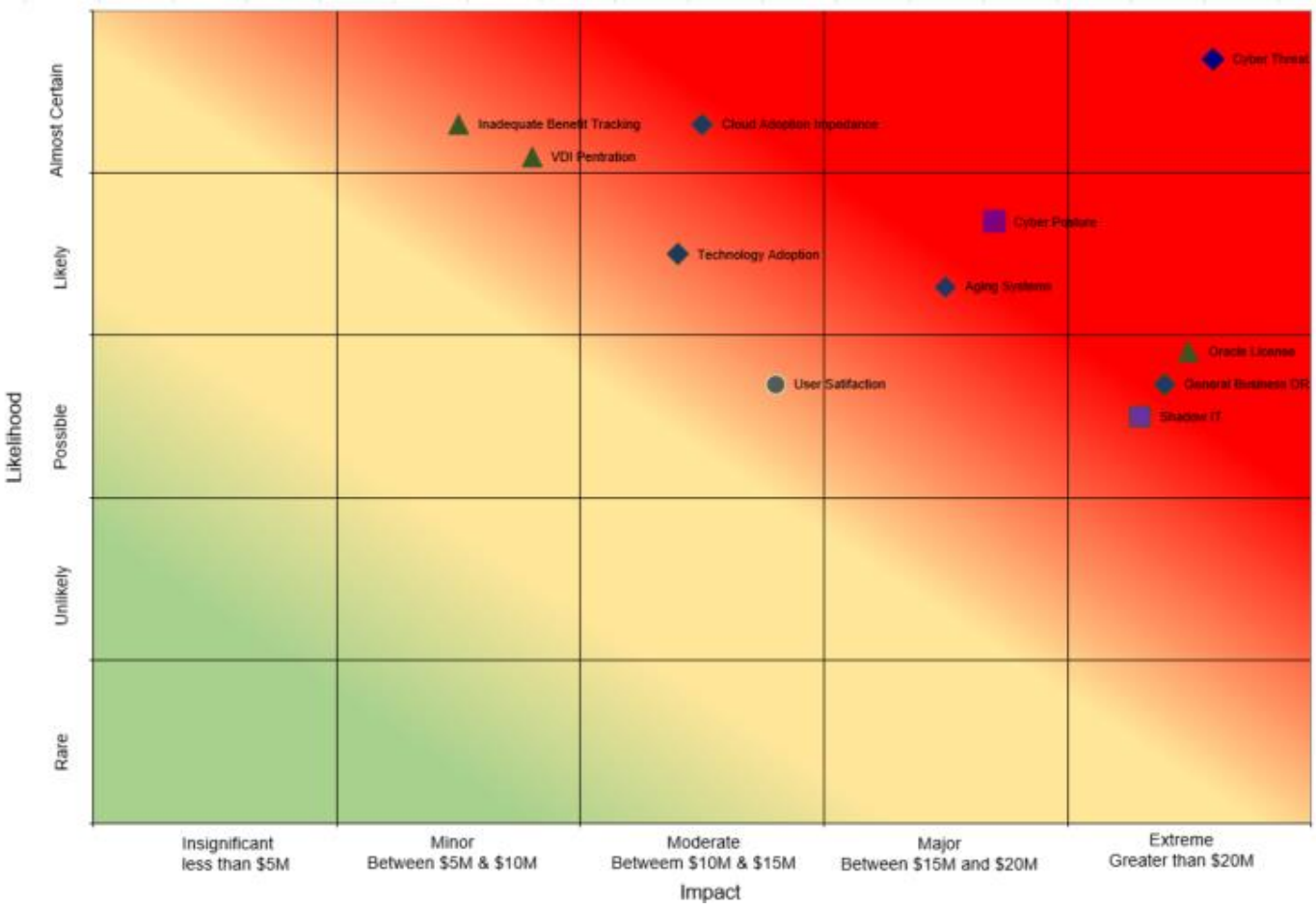
Table 9.0-1 identifies IT risks in the five categories, along with their likelihood and consequence as defined by the framework, followed by heat maps to provide graphical representations. Again, IT has more interaction with reliability, financial, and compliance, and less with safety and environment.

### *Table 9.0-1 IT Risk Assessment*

| Risk Category | Risk Name: Risk Description | Likelihood | Impact |
|---|---|---|---|
| Reliability | **Cyber Threat:** During a risk identification workshop, project SMEs identified 12 distinct cyber security risks. The risks include 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. Three of the risks are 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<br>Financial | **Cloud Adoption Impedance:** Combination of:<br>• Incomplete understanding of interface complexities, dependencies, and/or business value.<br>• 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.<br>Leads to:<br>• Failing to develop/adopt cloud native solutions resulting in increased cloud migration risks and costs.<br>• Slow adoption of cloud-based solutions resulting in end user dissatisfaction (end users attempt to contract SaaS outside of IT with an associated increase in security risks and costs). | Almost Certain | Moderate |

| Risk Category | Risk Name: Risk Description | Likelihood | Impact |
|---|---|---|---|
| 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 leverage cloud for business system Resiliency leads to a large capital investment by facilities to build data center and by IT to populate the data center with network gear, servers, and storage to support General Business System Resiliency. | Possible | Extensive |
| 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 | Extensive |
| 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:<br>• Much higher expense costs in the IT budget to obtain and retain staff.<br>• Inability to attract appropriate skill levels. | Certain | Moderate |
| Safety Reliability | **On-the-job Injuries:** IT workers are injured while in duty status due to:<br>• Travel accidents<br>• Slips, trips, or falls<br>• Installation of electronic IT equipment<br>• Repetitive ergonomic maladies<br>Leads to:<br>• Insufficient staff to meet operational requirements<br>• Delays to project schedules resulting in lower financial benefits | Possible | Minor |
| Safety Reliability | **COVID Exposure:** IT workers contract COVID, leading to insufficient staff to meet operational requirements and delays to project schedules resulting in lower financial benefits. | Likely | Major |
| Financial | **Contract Inflation:** Maintenance contracts for IT products and services continue to outstrip national economic inflation rates leading to increased cost pressure on IT expense budgets. | 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. | 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). | Certain | Moderate |

*Figure 9.0-1 Risk Assessment*




## 10.0 STRATEGY AND FUTURE STATE

The current direction for the Agency is that rates, and therefore IPR requests, shall remain flat or below inflation overall for the next several years. However, this IT strategic asset management plan is intended to describe and plan for what is needed to both maintain the products and services currently in use according to their individual life cycle characteristics, as well as to identify known emerging IT product and service requirements as expressed by IT's business clients. It is not a budget exercise concerning the IT organization's budget or resources. While the capital planning information can translate directly to the Integrated Program Review, the expense information included in this plan does not encompass the entirety of IT's expense needs.

BPA should adopt an overall IT Strategic Asset Management Plan that treats all of BPA as one entity with varying degrees of IT requirements. This one-BPA approach should not only encompass the day-to-day administrative environments that support common business functions with automation and IT technology, but also the specialized subset of IT that is used

to monitor and control real devices and operational environments, and is known as Operational Technology (OT). There are challenges with this approach: these two areas of IT have traditionally remained separate at BPA; the timeframe to accomplish this is too long to provide the appropriate level of detail and discernment prior to the publication of this rate period. For these reasons, the combination of IT and OT into a one-BPA strategic asset management plan is deferred to future cycles.

The IT Asset Strategy addresses two distinct set of assets, infrastructure and business applications, with separate characteristics and objectives. Infrastructure assets includes all information devices and management software needed to provide connectivity, computational capacity, storage as well as management software needed to host, operate, and secure applications to meet the business automation needs of the Agency. 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.

IT has dramatically reduced staff over the last several years, as well as reduced contractual obligations where feasible, to meet budget requirements. As a result, we have begun to experience increasing system outages and time to recover. 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 led to the deferral of life cycle activities for existing products and services in some cases, in favor of adding new capabilities. To address this issue, the strategy for IT is to:

- Transparently identify and publish the cost for all services characterized as core services provided by IT. For example, network connectivity, a personal computer service, general unstructured electronic storage, desk telephone service, enterprise applications for financial, asset management, human resources capabilities, etc.
- Maintain a layered approach to project prioritization that begins within the IT client business lines, and culminates in a cross-agency prioritization of the IT work plan, with final approval by the CIO.
- Prioritize core-sustainment life cycle activities over expansion efforts to the extent possible, with Critical Business Systems taking precedence over Enterprise Business Systems.
- Make every effort to identify current systems that are at life cycle risk, and get them back into alignment with their published refresh rates. This directly supports the agency strategic objectives of modernization and financial health.
- Negotiate an increased IPR expense portfolio that reflects realistic inflation rates for IT and acceptably mitigates primary barriers to successful management of IT assets:
    - Meet cyber security mandates, and maintain acceptable levels of cyber security protection.
    - Restore staffing levels to mitigate single-points-of-failure and service gaps. Drive the concept of Remote Work for IT positions, otherwise hiring appropriate skill sets and capabilities will not meet needs or even attrition replacement.
    - Meet technology directives from DOE or other federal bodies.
    - Advance identification and planning for customer project demand.

## 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 and enable those cost savings to be used to meet business needs.
  - Security and Risks
  - Reliability
  - Resiliency

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

## 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 | 3 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-2 of current vendor supported version (security/reliability) |

A recent sub-strategy employed to make sure that future desktop refresh cycles are maintained is to convert the assets from BPA-owned to leased assets. The lease must be paid, or the assets will be repossessed by the vendor. It is likely a similar approach will be adopted for mobile phones. There is also a possibility that the same approach may be taken with server and/or network components as well, if the cost of lease vs ownership is as much in favor financially as it was for the desktops assets. Migration to subscription-based Software-as-a-Service is similar in nature and has already begun in several locations.

Consolidation and virtualization of data center components over the last several years has allowed IT to reduce its production data center footprint to a level that the enterprise business systems could deploy a failover configuration into the alternate data center at Munro without having to build additional facilities. Moving to an annual percentage refresh cycle for data center assets allows IT to rotate equipment to the failover function, then test, then development environments. This sustainment rotation will enable the resiliency objective for most if not all systems from an infrastructure perspective, to meet the requirements laid out in the recent Business Impact Analysis Report for Enterprise Business Systems.

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.

The process and method for prioritizing sustain projects is not expected to change from what was described in section 7: 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.

### 10.2.2 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

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, 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 leveraging existing advances in consolidation and virtualization of the data center, and adding 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.
- Determnation 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 me 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.

Technological changes are expected, and in fact do, arise between lifecycle 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.

## 10.3 Planned Future Investments/Spend Levels

As can be inferred from the table, IT has a strong sense of the sustain funding required to maintain those assets that are already in production, and the few requests for new assets that we already know about. Historical experience indicates that IT's business line partners often generate requests for major application expansion efforts on a much shorter timeframe than the two years and beyond examined during the IPR process. This requires IT to be somewhat dynamic in planning for future investments. To that end, IT must use historical information to estimate future requests.

In addition to that, there are other pressures that influence the type of funding, capital or expense, that may be needed for any specific effort. 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.

From a historic perspective, spending reduction efforts within BPA resulted in lower than planned IT capital spend in FY17 through FY19. FY20 and FY21 returned to the levels of capital spending in IT typically encountered, in fact above largely as a result of GridMod and EIM enterprise efforts, and this leads IT to plan for similar levels for FY24 and FY25.

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

1) Unknown capital expand project requests historically 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 FY22 and FY23.
3) The Capital Sustain in 2024/25 includes possible expenditure for building out the new Vancouver Control Center building, and migrating the HQ data center there.
4) Capital Sustain in FY27/28 includes possible replacement of the entire ERP stack. This is completely notional at this time.
5) While we have no detailed information at this time, we expect an effort to modernize Financial systems to begin in FY24 (FinMod).
6) Table 10.3-1B is added to clarify the breakdown of OpEx funding required in order to execute on the capital portfolio.

***Table 10.3-1A Future Capital Expenditures (in thousands)***

| Program | Rate Case FY's | | Future Fiscal Years | | |
|---|---|---|---|---|---|
| Capital Expand (CapEx) | 2024 | 2025 | 2026 | 2027 | 2028 |
| Apps | $7,125 | $8,000 | $2,500 | $0 | $0 |
| Data Center | $127 | $350 | $0 | $0 | $0 |
| Networks | $0 | $0 | $0 | $0 | $0 |
| Office Automation | $0 | $0 | $0 | $0 | $0 |
| Expected Unknown Requests | $0 | $0 | $8,670 | $2,066 | $2,454 |
| **Total Capital Expand** | $7,252 | $8,350 | $11,170 | $2,066 | $2,454 |
| Capital Sustain | 2024 | 2025 | 2026 | 2027 | 2028 |
| Apps | $3,800 | $1,700 | $3,100 | $10,000 | $10,000 |
| Data Center | $4,612 | $4,675 | $2,241 | $2,308 | $2,377 |
| Networks | $6,336 | $6,526 | $6,722 | $6,924 | $7,131 |
| Office Automation | $1,100 | $1,133 | $1,167 | $1,202 | $1,238 |
| **Total Capital Sustain** | $15,848 | $14,034 | $13,230 | $20,434 | $20,746 |
| **Total Capital** | $23,100 | $22,384 | $24,400 | $22,500 | $23,200 |

*Table 10.3-1B Future Expense Expenditures (in thousands)*

| Program | Rate Case FY's | | Future Fiscal Years | | |
|---|---|---|---|---|---|
| Expense to Execute Cap Expand | 2024 | 2025 | 2026 | 2027 | 2028 |
| Initial Investment (80% of 10%) | $580 | $668 | $894 | $165 | $196 |
| Net New O&M (20%) | $1,450 | $1,670 | $2,234 | $413 | $491 |
| **Total** | $2,030 | $2,338 | $3,128 | $578 | $687 |
| Expense to Execute Cap Sustain | 2024 | 2025 | 2026 | 2027 | 2028 |
| Initial Investment (20% of 10%) | $317 | $281 | $265 | $1,226 | $1,245 |
| Net New O&M (3%) | $475 | $421 | $397 | $613 | $622 |
| **Total** | $792 | $702 | $662 | $1,839 | $1,867 |
| Exp-only Expand and Sustain | 2024 | 2025 | 2026 | 2027 | 2028 |
| Project (80%) | $3,644 | $937 | $1,840 | $1,280 | $1,200 |
| Net New O&M (20%) | $729 | $187 | $368 | $256 | $240 |
| **Total** | $4,373 | $1,124 | $2,208 | $1,536 | $1,440 |
| Grand Total | $7,195 | $4,164 | $5,998 | $3,953 | $3,994 |

## 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 notbe met, possibly leading to increases 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 notbe met, possibly leading to increases 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 cos 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.

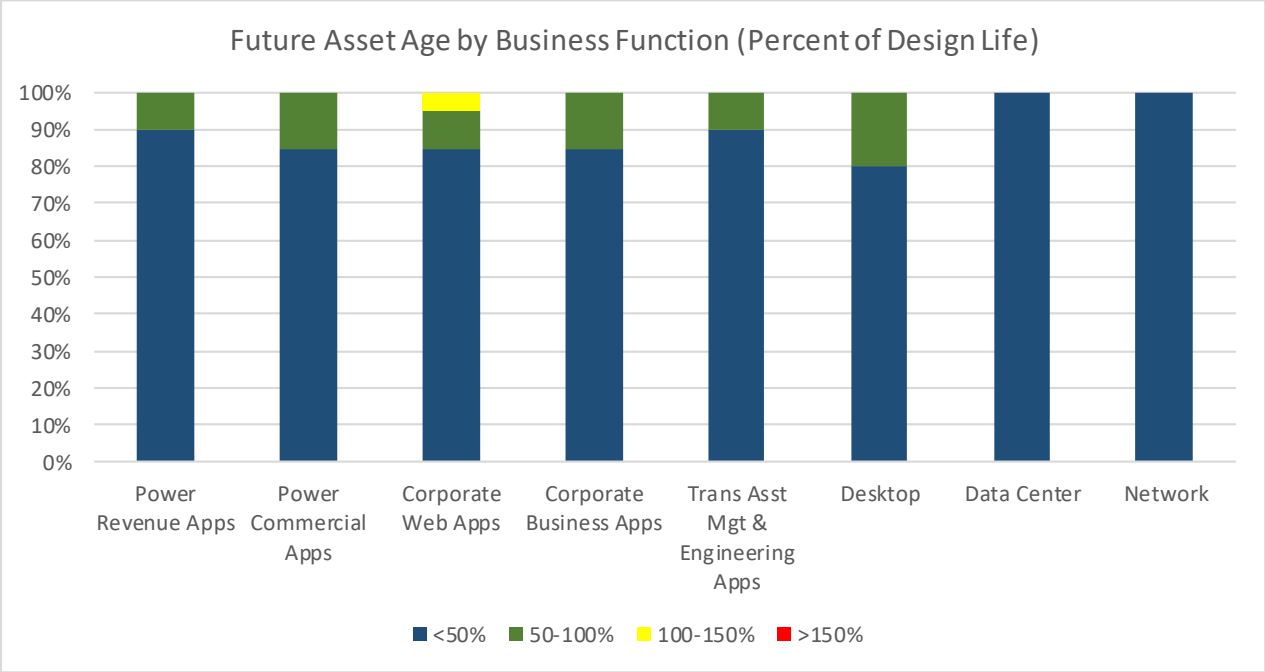



*Figure 10.5-1 Future Asset Age by Business Function*

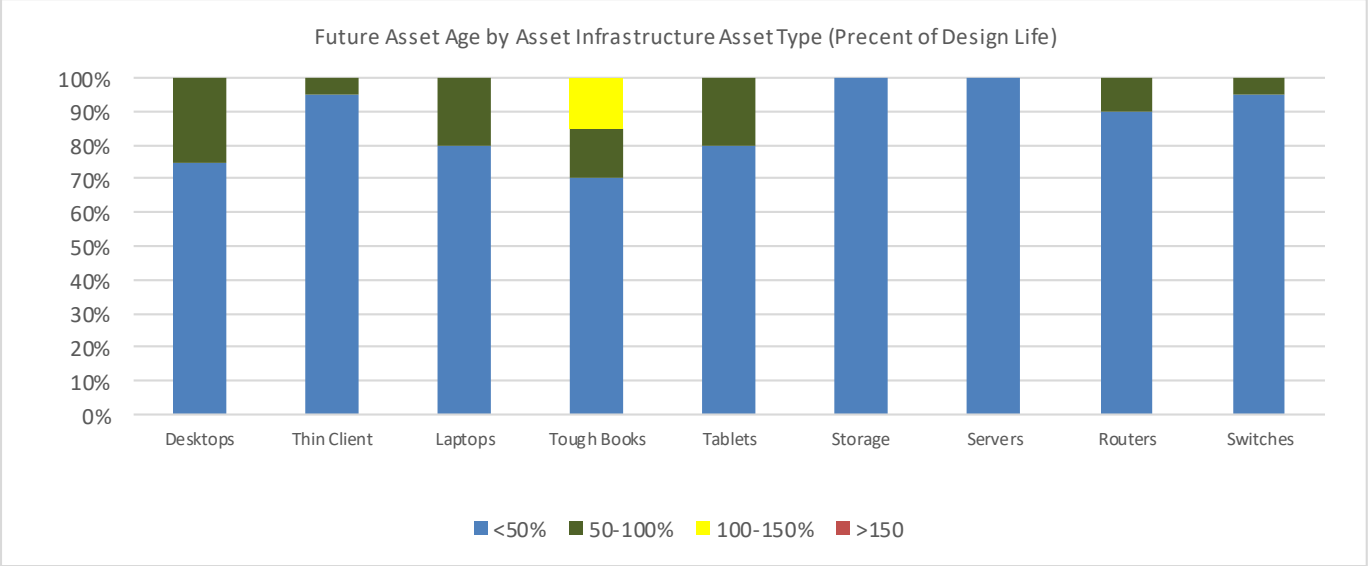



*Figure 10.5-2 Future Asset Age by Asset Type*

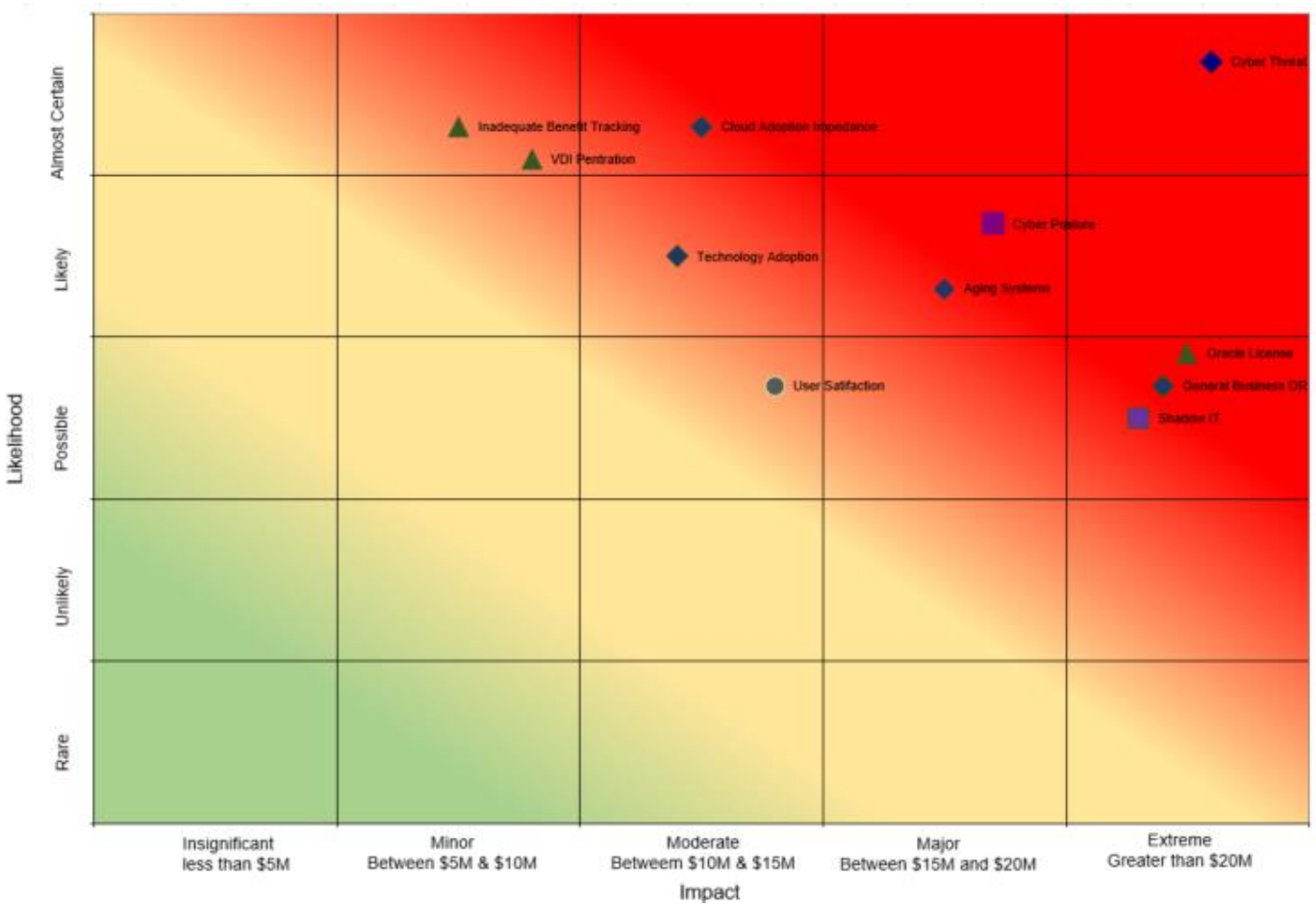
## 10.6 Performance and Risk Impact

### *Table 10.6-1 Sustain-only Strategy, IT Risk Assessment*

| Risk Category | Risk Name: Risk Description | Likelihood | Impact |
|---|---|---|---|
| Reliability | **Cyber Threat:** During a risk identification workshop, project SMEs identified 12 distinct cyber security risks The risks include 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. Three of the risks are 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 FY2013 Cyber Security Strategic Plan. | Almost Certain | Extreme |
| Reliability<br>Financial | **Cloud Adoption Impedance:** Combination of:<br>• Incomplete understanding of interface complexities, dependencies, and/or business value.<br>• 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.<br>Leads to:<br>• Failing to develop/adopt solutions cloud native applications resulting in increased cloud migration risks and costs.<br>• 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 |
| Financial | **VDI Penetration**: Inadequate inventory of hardware and software coupled with incomplete understanding of business usage leads to lower thin client penetration and failing to achieve full business value from Virtual Desktop Infrastructure (VDI). | Almost Certain | Minor |
| Compliance | **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<br>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<br>Financial<br>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 | Extreme |
| Reliability<br>Financial | **General Business System DR**: Failure to leverage cloud for business system Disaster Recovery (DR) leads to a large capital investment by facilities to build data center and by IT to populate the data center with network gear, servers, and storage to support General Business System DR. | Possible | Extreme |
| Financial | **Oracle License**: Loss or major modification of J's 20-year 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 |

| Risk Category | Risk Name: Risk Description | Likelihood | Impact |
|---|---|---|---|
| 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 |

*Figure 10.6-1 Sustain-only Strategy, Risk Assessment*




## 11.0 Addressing Barriers to Achieving Optimal Performance

The practice of Asset Management is at varying levels of maturity within IT. The use of the Project and Portfolio Manager (PPM) software to house IT asset plans has proven unwieldy and caused service managers to forsake their asset plan documentation. We have been reverting to a standardized spreadsheet approach until such time as a formal asset plan management platform is chosen by the agency.

Over the last two years, IT has shortened refresh rates to adopted industry best practice to refresh infrastructure and personal computing devices on a three-year cycle. 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.

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.

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 has been partnering to build the practice of developing metrics to track applications' business benefits. The intent is 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.

In FY2017 IT initiated 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.

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 remote work at the agency is resulting in lower applicant levels, hiring offers turned down, and failed recruitments.

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.

# 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 additional 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 lines and substations.