FLORIDA
DEPARTMENT of
CORRECTIONS

Governor
RON DESANTIS
Secretary
RICKY D. DIXON

501 South Calhoun Street, Tallahassee, FL 32399-2500

www.dc.state.fl.us

October 15, 2023

The Honorable Doug Broxson
Chair, Senate Committee on Appropriations
201 The Capitol
404 South Monroe Street
Tallahassee, Florida 32399

The Honorable Thomas Leek
Chair, House Appropriations Committee
221 The Capitol
402 South Monroe Street
Tallahassee, Florida 32399

Mr. Chris Spencer, Director
Office of Policy and Budget
400 S Monroe St.
Tallahassee, FL 32399

Florida Digital Service
Mr. Pedro Allende, Secretary
Florida Department of Management Services
4050 Esplanade Way
Tallahassee, FL 32399

RE: Cloud First Strategic Plan

Dear Chair Broxson, Chair Leek, Director Spencer and Secretary Allende,

Please find the attached report per Section 282.206, Florida Statutes, using the strategic planning template provided by the Department of Management Services for both the Florida Department of Corrections (FDC) and the Florida Commission on Offender Review (FCOR). The document contains all planning information requested from the "Application Cloud Strategic Plan Guidance and Summary Template" developed by the Department of Management Services as guidance for agency submission. The Department has also included separate, supporting documentation detailing an updated assessment on the inventory of applications for both FDC and FCOR.

Respectfully,

Ricky D. Dixon
Secretary

FLORIDA DEPARTMENT OF CORRECTIONS

Office of Information Technology

APPLICATIONS CLOUD FIRST

STRATEGIC PLAN

October 15, 2023

Contacts

Chief Information Officer		Deputy CIO, Technology Solutions	
Ruth Lang		**Greg Prescott**	
Phone:	850-717-3963	**Phone:**	850-717-3895
Email:	Ruth.Lang@fdc.myflorida.com	**Email:**	Greg.Prescott@fdc.myflorida.com

Deputy CIO, Infrastructure and Operations		Program Manager	
Coleman Ayers		**Richard Lewis**	
Phone:	850-717-3283	**Phone:**	850-717-3617
Email:	Coleman.Ayers@fdc.myflorida.com	**Email:**	Richard.Lewis@fdc.myflorida.com

Table of Contents

Tables

Figures

1 Executive Summary

In 2019, the Florida Department of Corrections (FDC, Department) adopted an Applications Cloud Strategic Plan as required by F.S. 282.206, section 4. The Department's vision presented in this report is to conduct its operations and business via digital methods, using applications, connectivity and infrastructure, and contracted services to operationalize this vision.

The Department is embarking on this transformation from deep technical debt in each of the critical areas that support this vision. A statewide, national, and even global view of its mission required highly scalable, available, innovative, and elastic infrastructures and technology platforms. FDC leadership embraces this vision, and along with the State's Cloud-first policy (F.S. 282.206), the Department is assured that public cloud computing services and capabilities are crucial to support the Department's strategic technology requirements.

Technology is constantly emerging and changing how governments interact with constituents. Cloud computing enables the achievement of the business goals that are statutorily the mission of FDC. There are four-phases to the Department's strategy. It begins with lift and shift of applications and database servers from the State Data Center to the cloud, restoring mission critical and other business applications that are end-of-life, restoring and modernizing other business applications that are end-of-life, and requesting recurring funds for a continual annual refresh of application technology.

This strategic direction is preferred to realize the following cloud drivers, generated in conjunction with broader organizational goals and in pursuit of the overall IT strategy:

1.1 Business Goals

- All workloads will migrate to the public cloud where possible, with PaaS and IaaS as alternative options where SaaS is inappropriate.
- SaaS will be the primary service model.
- Accelerate the decommissioning of FDC resources in existing data centers, such as the State Data Center.
- Become more innovative, agile, and responsive to business demands by reducing the time to deployment of new projects.
- Build connectivity across all FDC facilities and maintain a current inventory of status.
- Develop recurring budgets and plans to refresh technology capabilities.
- Improve FDC's ability to react and respond to scaled requirements.
- Implement connectivity initiatives across FDC Institutions and Community Corrections to deploy applications and programs to staff, inmates, and offenders.
- Establish a statewide and national footprint without the need for capital investments.

1.2 Benefits

- Faster response to changes within the demands of the correctional system and mission.
- Faster time to deploy business initiatives for applications and programs.
- Increased productivity by shifting IT staff away from legacy platforms to higher-valued environments.
- Support for new business initiatives, such as leveraging AI, Machine Learning, Internet of Things (IoT), data warehouse and its advantages, data analytics using BI tools, microservices, and other innovative modern technologies that are not possible within the current environments.
- Reduce the time to access and use new technologies as released from cloud providers, shortening the wait of the release cycles.
- Significantly improving availability, security, access, to FDC applications with greater reliability and secured architectures from cloud providers.

- Deploy disaster recovery and business continuity with failover capabilities that are not currently available to support the Department in outage scenarios that affect officer and inmate safety.
- Increase reaction to scalability as resources are available on demand without human intervention to manage and forecast capacity.

1.3 Financial Commitment

To ensure that this overall vision is executed effectively, this strategy requires funding on par with the Department's overall role in public safety, scale of responsibilities, and areas of technical debt. Each of these components is critical to understanding how FDC will succeed in the cloud, mitigate risks, and prepare staff and users for the transition.

The four broad areas identified to successfully transition to the cloud will each require initial and recurring funding commitments. Summarizing these commitments requires alignment in four broad areas: Applications, Connectivity, Infrastructure, and Contracted Services.

1.4 Recommendations

The Department recommends the four-phased approach to realize the vision of applications that enable the fulfillment of its statutory responsibilities. Systems that are not vulnerable to security threats, efficiently and fully support Institutions, Community Corrections, and Programs and Administration. Realizing the envisioned state and operational outcomes of the Department's cloud-first strategy depends on support for the phases identified along with the requested funding.

2 Introduction

The Florida Department of Corrections (FDC, Department) updates and submits the Cloud Strategic Plan (CSP), by October 15 each year, as required by Florida Statute (F.S.) 282.206(4). The plan is submitted to the Office of Policy and Budget in the Executive Office of the Governor and chairs of the legislative appropriations committees. Additionally, an electronic copy of the plan is submitted to the Florida Digital Services FL[DS].

Since 2019, the Department submitted the CSP that includes both the Florida Department of Corrections and the Florida Commission on Offender Review (FCOR). The 2023 submission continues this approach.

The 2023 CSP continues to follow the Department of Management Services (DMS) template. It does not repeat the structure of prior submissions. The Department is actively pursuing the strategy documented and presents the information that operationalizes the CSP.

For the reader's convenience, terms and definitions are provided at the end of this document and a review of our current state is provided.

2.1 Cloud Computing Baseline

To ensure that stakeholders and readers have a consistent understanding of the CSP, relevant terms associated with the strategy are identified and described below.

1. **Azure Government Cloud** is a cloud computing platform provided by Microsoft specifically designed to meet the unique and stringent requirements of government agencies and organizations in the United States. It offers a secure and compliant cloud environment that adheres to government regulations, including FedRAMP (Federal Risk and Authorization Management Program) High and Moderate impact levels, HIPAA (Health Insurance Portability and Accountability Act), and DoD (Department of Defense) Impact Level 5. Key features of Azure Government Cloud include:
    - **Data Residency:** Data is stored within the United States, ensuring that sensitive government information remains within the country's borders.
    - **Compliance:** Azure Government Cloud adheres to numerous compliance standards, making it suitable for federal, state, and local government agencies, as well as contractors working with the government.
    - **Security:** It provides robust security measures to safeguard data, including encryption, threat detection, and continuous monitoring.
    - **Availability:** Azure Government Cloud is designed for high availability and reliability, ensuring that government services can operate without interruption.
    - **Scalability:** Government agencies can scale their IT resources as needed, allowing them to adapt to changing demands.
    - **Hybrid Capabilities:** It supports hybrid cloud deployments, allowing agencies to integrate their on-premises infrastructure with the cloud for a seamless and efficient IT environment.

3 Scope

The scope of the CSP addresses the Department's inventory of applications located at the state data center. In addition, the plan includes the following elements:

- **Readiness:** The plan should identify and document the readiness of each application for transition to a cloud computing service.
- **Appropriate strategy:** The plan should outline the appropriate strategy for transitioning each application to a cloud computing service.
- **High-Level Timeline:** The plan should provide a high-level timeline for the transition of each application to a cloud computing service.
- **Quality, Cost, and Resource Requirements:** The plan should be based on the quality, cost, and resource requirements of applications.

The Department understands that the purpose of the plan is to assist the state data center in adjusting its service offerings (Section 282.206(4)).

3.1 Business Baseline

Chapter 20.315 established the Florida Department of Corrections to protect the public through the incarceration and supervision of offenders and to rehabilitate offenders through the application of work, programs, and services.

The Department operates the third largest state prison system in the country with an annual budget of over $3.3 billion. FDC is the largest state agency in Florida, with over 22,000 employees and approximately 89,000 inmates incarcerated. The FDC also supervises nearly 146,000 offenders on community supervision.

The Department meets its mission objectives by providing a variety of programs and services to inmates and offenders, including educational, vocational, and substance abuse treatment programs. The FDC also works with community partners to provide support and resources to offenders after they are released from prison.

Chapter 945, Florida Statutes (F.S.) establishes the business baseline objectives for the Department, which include:

1. **Public Safety:** FDC alongside other state agencies plays a crucial role in ensuring public safety by securely confining individuals who pose a threat to society. This includes those convicted of serious crimes and individuals awaiting trial or sentencing.
2. **Offender Programs:** FDC offers a range of educational, vocational, and treatment programs to help offenders acquire new skills and address underlying issues such as substance abuse and mental health. These programs are designed to increase the chances of successful reintegration into society upon release.
3. **Parole and Probation:** FDC oversees parole and probation services for eligible offenders, providing supervision and support to help them reintegrate into the community while ensuring compliance with the conditions of their release.
4. **Victim Services:** FDC has victim services programs to assist and support the victims of crimes, including providing information on the status and release dates of offenders.
5. **Security and Administration:** FDC maintains secure and well-administered correctional facilities, ensuring the safety of both staff and inmates. This includes managing the day-to-day operations of these institutions. Administering the vast and complex services that must adhere to confidentiality of inmate

information and records, capabilities to enable restitution and other payments by inmates, education, and testing of inmates on communicable diseases, and involuntary mental health treatment of inmates.

3.1.1 Organization

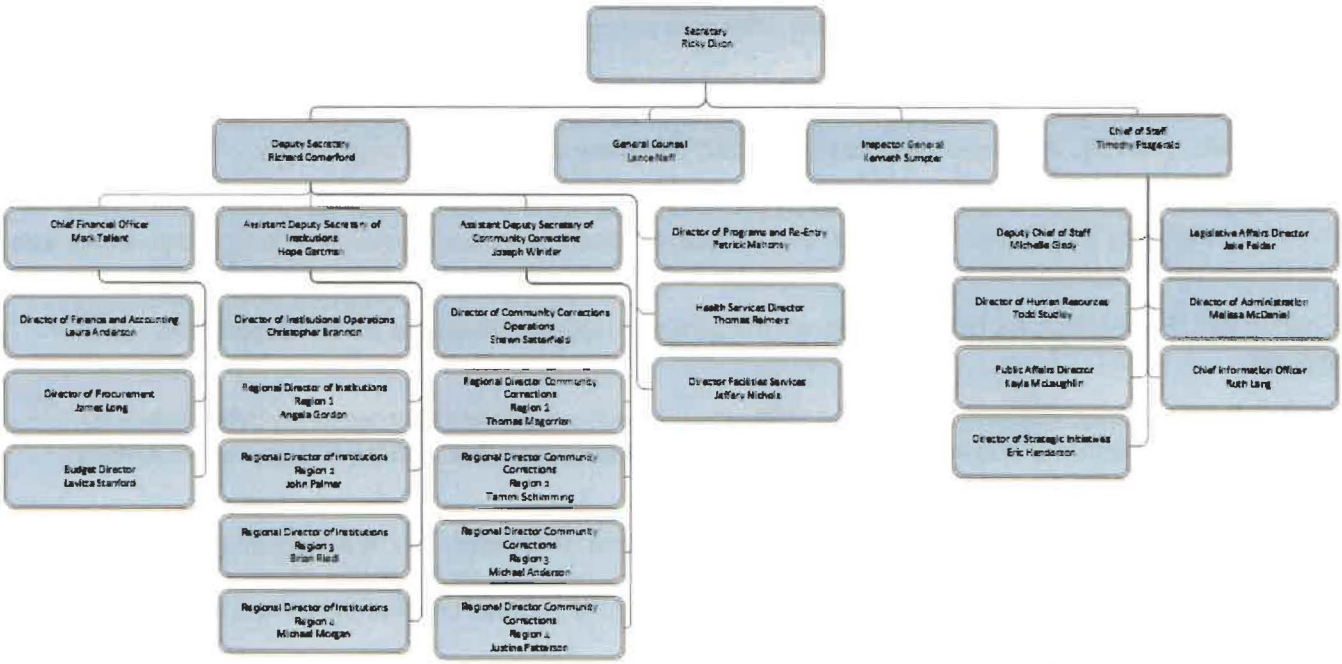
The FDC organization chart structure provides a visual depiction of the business scope that the cloud strategy must support. The Department led by the Secretary of Corrections, appointed by the Governor, and confirmed by the Senate. The Secretary is responsible for the overall operation of the Department and reports to the Governor. There are **two** main operating divisions in the Department: **Institutions** and **Community Corrections**.

The **Institutions** division is responsible for overseeing the state's 50 correctional institutions. Institutions include prisons, work camps, and re-entry centers. Programs and services, aim to rehabilitate and reduce recidivism. Technology infrastructure, connectivity, and applications are essential to achieving operational outcomes.

The **Community Corrections** division is responsible for overseeing the state's 67 probation offices and their associated support functions. Inmates transitioning towards release and offenders are the focus of Community Corrections operations. Technology is also critical for delivering offender programs and workforce capabilities.

Below is the FDC organizational chart. Technology infrastructure and connectivity, applications, security, and IT services staff are critical for the efficient functioning of each layer of the organization.

Table 1: *FDC Organization Chart*



In addition to Institutions and Community Corrections, there are **several** administration organizations responsible for departmental administrative operations. Technology capabilities and services are critical across every level of the FDC organization and operations.

3.1.2 Benefits of the Cloud

Benefits from the adoption of the cloud align with the scope, complexity, security, and availability requirements that the Department must adhere to by statute. Given the size, complexity, and statewide needs, technology specifically software applications, connectivity, and contracted technology services provide the platforms to every operating entity statewide.

Operations in each institution and correctional facility use the same systems which must comply with strict federal and state laws. The cloud platform provides the means to economically achieve the above listed benefits, while allowing innovation and avoiding technical debt. The six elements of the cloud computing baseline noted above shifts the burden from maintaining and investing in home grown technologies that are increasingly difficult to support.

3.2 REQUIREMENTS

The Cloud First Strategic Plan aligns with the Department's business objectives and provides the context to justify the cloud strategy. Selection of the cloud strategy is to enable achieving the continuous support for successful business operations, innovation, and security. Applications, infrastructure and connectivity, cybersecurity, and staffing are the major areas of technology capabilities to support the delivery of operational services. These four areas are the focus of the CSP.

Summarizing the technology objectives that provide capabilities and support business objectives are described in the tables below. The tables identify CSP objectives in four areas: infrastructure and connectivity, applications, cybersecurity, and staffing through contracted services. Following are three tables that describe the four objectives.

Table 2: *Critical Infrastructure and Connectivity Objectives of the Cloud Strategy*

Infrastructure Objectives of the Cloud Strategy		
#	**Objectives**	**Criticality**
1.	Provide infrastructure management tools that protects against cyber-attacks and infrastructure and connectivity performance that result in rapid information flow impacting improved public safety.	Critical
2.	Provide connectivity to buildings to access cloud services that enable inmate access to education and re-entry program offerings, and with the capacity to install monitoring and security devices that support officer and inmate safety.	Critical
3.	Provide technology equipment refresh for aging network components including servers in field locations, officer tablets, workforce laptops, monitors, and desktops that will support current and newer cyber security tools to protect against hackers and the exploiting of other vulnerabilities.	Critical
4.	Provide network redundancy with failover to ensure continuous traffic when portions of the network fail that better secures the workforce during system failures and provision continuous support during law enforcement and public safety events.	Critical
5.	Provide cybersecurity organizational competencies that is standard for the Department and its high security responsibilities.	Critical
6.	Provide baseline contracted services that begins to shift the Department to maintain services to thousands of users resulting in responsiveness and better quality allowing the workforce to deliver the level of services to all constituents and public safety partners.	Critical

Infrastructure Objectives of the Cloud Strategy		
#	**Objectives**	**Criticality**
7.	Provide contracted services that focuses on modernizing the Department's infrastructures, demanded by the pace of technology changes, while allowing the Department to meet its crucial responsibilities while ensuring public safety.	Critical

Table 3: *Critical Applications Objectives of the Cloud Strategy*

Applications Objectives of the Cloud Strategy		
#	**Objectives**	**Criticality**
1.	Provide replacement for critical and end-of-life software applications and backend application infrastructures that if not addressed will impact interfaces and data exchanges with law enforcement and public safety responsibilities.	Critical
2.	Provide re-engineered applications to rebuild existing software systems that are nearing end-of-life and require feature upgrades to respond to data requirements and effectively support public safety partners.	Critical
3.	Provide applications that are built to support deployment on mobile devices.	Critical
4.	Provide applications that are securely deployed via web and mobile device applications interfaces to support inmate and offender education, counseling, and readiness to return to communities.	Critical
5.	Provide contracted services that focuses on modernizing the Department's applications, demanded by the pace of technology changes, while allowing the Department to meet its crucial responsibilities.	Critical
6.	Provide and sustain an applications environment and practice around cybersecurity that relies on strong cryptographic applications management capabilities that are hardened against inmate hacking.	Critical

Table 4: *Critical Cybersecurity Objectives of the Cloud Strategy*

Security Objectives of the Cloud Strategy		
#	**Objectives**	**Criticality**
1.	Provide infrastructure management tools that protects against cyber-attacks and infrastructure and connectivity performance that result in rapid information flow impacting improved public safety.	Critical

Security Objectives of the Cloud Strategy		
#	**Objectives**	**Criticality**
2.	Provide platforms that are CJIS compliant and support the current release version 5.9.1 or the most current.	Critical
3.	Provide capabilities that comply and support Chapter 60GG-4.004 – Cloud Security and Risk Mitigation Strategy.	Critical
4.	Provide capabilities enforcing multi-factor authentication	Critical
5.	Support the additional requirements in the section on **Security and Risk Planning**	Critical

4 Current Situation

In 2023, OIT assessed the state of Departmental technology systems in applications and connectivity, and contracted services. Findings showed significant and several critical needs impacting operational reliability, efficiency, and the ability to innovate. Applications and systems supporting Institutions, Corrections, and related program areas were at critical points of failure, lacking capacity, and no connectivity across 25% of the complex of facilities. In each technology area, findings showed the common impact of technical debt, i.e., reduced quality, increased costs, slower development, and insufficient budget allocation.

4.1 INFRASTRUCTURE

Current state of the infrastructure consists of aging non-supported hardware and software. This results in an overall lack of staff productivity and presents significant information security risks. An IT infrastructure needs to keep pace with the ever-changing requirements from the user community and be able to make use of the latest innovations in technology to provide efficient and effective solutions.

Lack of identified continued funding for replacement and upgrades has resulted in an operating environment where nearly half of the 13,000 workstations and more than half of the 84 file and print servers in use are at end of life (EOL).

Uninterruptable Power Supplies (UPS) are an integral part of ensuring a computing environment availability. In the event of a power interruption, these devices provide a level of support that allows an orderly shutdown of equipment and protects against power surges. The lack of these devices exposes data servers and phone systems to possible damage Currently, 50% of UPS in use are over 10 years old and are not cost efficient to repair.

With the lack of fiber connectivity between buildings and locations. The utilization of legacy copper connectivity impedes communications, slows transmission of data, and decreases employee productivity. Below is a list of infrastructure findings:

Devices supported and Deficient Connectivity:

- 84 field File and print servers EOL (hardware)
- 13 Data Center servers EOL (Software)
- 127 field and data center servers approaching software EOL (10 October 2023)
- 13,191 FDC Staff workstation/laptops (many are past EOL)
- No Network redundancy
- Insufficient network monitoring tools
- Server replacement need lifecycle refreshment
- Lack of fiber connectivity to sites and between buildings

The lack of connectivity affects:

- Operational capabilities
- Expansion of officer and inmate services

Table 5: *FDC Building Connectivity Status*

Summary of Connectivity Across FDC Buildings							
	Total Buildings	Connected	Not Connected	Not Connected (GTL)	Not Connected (Officer Stations)	Not Connected (Education)	Not Needed
Buildings	2,206	1,065	545	360	50	85	101

The Department prioritizes connectivity for the four areas marked in red. Connectivity requires several components, including installing fiber, installing network devices, addressing structural issues, conforming with physical security concerns, environmental concerns, and end user access and usability.

4.1.1 Aging and Unsupported Infrastructure Hardware and Software

File and Print Servers at facilities are obsolete and rapidly approaching their Operating System (OS) end of life dates. OS upgrades require more capable processors, which are not available on existing older model servers.

- Current network speeds at many facilities preclude the use of cloud (SaaS) options for housing data.
- Local servers are used to house operational documents as well as videos, requiring substantial storage.
- Distributed servers provide authentication services and access to external resources.
- Increased emphasis on digitization of records and criminal justice documents require investment in storage capacity that support document management standards.
- Central data store (Isilon), located in the data center, has configuration issues which prevent adequate auditing by FDC to maintain CJIS compliance; all audits must be requested from NWRDC. These issues impact multiple agencies and cannot be rectified without essentially performing a complete rebuild and reconfiguration of the system.

Table 6: *Aging Application Servers and Databases*

Operating System Age	Count	SQL Servers Age, Versions, and Count		
Year	**Count**	**Year**	**Version**	**Count**
2003	7	**2003**	SQL 2003	3
2008	6	**2008**	SQL 2008	3
2012	64	**2012**	SQL 2012	21
2016	43	**2016**	SQL 2016	11
2019	70	**2019**	SQL 2019	25
2022	17	**2022**	N/A	0
Linux	13	Linux	0	0

Operating System Age	Count	SQL Servers Age, Versions, and Count		
Year	**Count**	**Year**	**Version**	**Count**
Total	**220**	**Total**		**63**

Network monitoring software is a composition of opensource tools to monitor the network and servers (Nagios, Cacti, and an in-house written ping tool). Due to funding limitations, commercial tools were not purchased, and licensing for SolarWinds was removed.

4.2 APPLICATIONS

Current state of applications showed significant and critical needs impacting operational reliability, efficiency, and the ability to innovate. Applications and systems supporting Institutions, Corrections, and related program areas were at points of failure and lacking capacity to innovate using modern software platforms.

The agency has over 137 applications related to inmate and offender management and 70% of these are considered legacy because the hardware or software used is at or beyond end-of-life. By the end of 2026, 100% of the applications will be end-of-life if not updated.

Critical to the Department's mission is 37 applications, meaning that efficient workflow of inmate processing, inmate care, and inmate security could be gravely affected by an application crash. Reverting to manual processing and handwritten calculations will result in increased frustration for officers and inmates as services to inmates are reduced or delayed that result in safety concerns. A count of the EOL applications and business areas that will be impacted is provided below:

- 48 applications at EOL will affect Inmate general functions.
- 15 applications at EOL will affect Inmate Health.
- 4 applications at EOL will affect Inmate Finance and Money
- 20 applications at EOL will affect Inmate Security.
- 3 applications at EOL will affect Offender Monitoring.
- 5 applications at EOL will affect Inmate Food and Water.
- 6 applications at EOL will affect Officer Safety.

4.3 STAFFING AND BUDGET

Staffing is insufficient to provide quality IT Services at scale. Therefore, levels of services and service quality are impacted resulting in overdue responses to requests for services across all functional OIT areas. A comparison across state agencies in similar lines of business provides a compelling picture of FDC's deficient staffing.

Staffing levels, funding, and skills in software development aligned with contemporary technologies affects OIT, Institutions, Community Corrections, and administration areas. Delivering timely and quality IT services is delayed and not able to adhere to the service levels of OIT. Business areas suffer as applications and infrastructure services are not responded to timely.

Current state of staffing budget found that employee to IT staff support ratio at FDC, which is 128:1, was significantly lower than other similar Florida agencies. The average ratio for other Florida state agencies is 45:1.

With a significantly larger workforce, the impact is worse, as support staff moves through a larger population of users, before able to return to follow up work.

Table 7: *IT Services - Employee to IT Staff Ratio*

AGENCY	IT FTE	AGENCY FTE	STAFFING RATIO	IT STAFFING COMPARISON
Financial Services (DFS)	208	2,600	13:1	9x ↑
Highway Safety (DHSMV)	155	4,300	28:1	4x ↑
Juvenile Justice (DJJ)	60	3,200	53:1	2x ↑
Revenue (DOR)	182	5,000	27:1	4x ↑
Law Enforcement (FDLE)	118	1,900	16:1	8x ↑
Children and Families (DCF)	232	12,300	53:1	2x ↑
Corrections (FDC)	179	22,900	128:1	
		Average	45:1	

4.4 Staff Support Volumes

Staff support 39,000 devices, 29,000 employees, and respond monthly to 5,000 helpdesk calls, 3,000 e-mail requests, and 9,000 tickets. Staff capacity is critically low and needs to be significantly augmented to effectively manage and efficiently respond to the Department's users and stakeholders.

4.5 Budget

To support the October 15, 2023, CSP submission, the FDC IT budget references the Governor's Recommendations for the FY2023-2024 period.

Table 8: *Governor's Budget Recommendations*

Governor's Recommendation FDC, Information Technology Budget FY 2023-2024		
Policy Area: Information Technology	**Dollars**	**Positions**
Adjustments to current year estimated expenditures	**$1,942**	0
Total Agency-wide Information Technology	**$29,229,432**	
• Desktop life cycle management	$4,150,000	0
• Information technology infrastructure improvements	$200,000	0
• Offender Based Information Technology Modernization	$21,487,126	0
• Officer Station Network Connectivity	$3,392,306	0
Total Estimated expenditures	**$44,240,860**	
• Casualty insurance premium adjustment	$1,321	0
• Data processing assessment base budget adjustment	$0	0
• Estimated expenditures - operations	$43,517,093	179.5

Governor's Recommendation FDC, Information Technology Budget FY 2023-2024		
Policy Area: Information Technology	**Dollars**	**Positions**
• Florida retirement system adjustment - FY 2021-22 - normal cost and unfunded actuarial liability	$0	0
• Florida retirement system adjustment - FY 2022-23 - normal cost and unfunded actuarial liability (UAL)	$101,141	0
• Reallocation of human resources outsourcing	$0	0
• Salary increases FY 2022-23 - statewide $15 minimum wage increase - effective 7/1/2022	$1,153	0
• Salary increases FY 2022-23 - statewide 5.38% pay increase - effective 7/1/2022	$620,152	0
• Salary increases for FY 2021-22 - state employee minimum wage increase - effective 7/1/2021	$0	0
• State enterprise information technology distribution	$0	0
Total Inter-agency reorganizations - information technology	**$0**	
• Data processing services category - add	$0	0
• Data processing services category - deduct	$0	0
Total Nonrecurring expenditures	**($14,516,514)**	
• Desktop life cycle management	($1,000,000)	0
• Information Technology Infrastructure Improvements	($3,364,640)	0
• Information technology services provided to the florida commission on offender review	$0	0
• Offender based information technology modernization	($10,151,874)	0
Total Program or Service-Level Information Technology	**$116,000**	
• Information technology services provided to the Florida Commission on Offender Review	$116,000	0
Grand Total Policy Area: Information Technology	**$59,071,720**	**179.5**

Note: Data for FY 23-24 from Bolder Brighter Better Future
URL: BolderBrighterBetterFuture

Current state of the Department's budget does not scale with agencies in similar lines of business such as Florida Department of Law Enforcement and Department of Children and Families. The IT budget for the Department is 1.79% of its total budget. While increased in FY 23-24, budget does not align with supporting a staff of 23,120 and it does not fund IT positions.

Funding the CSP will allow the Department to build and deploy modernized applications. The new applications will be built on newer more contemporary software platforms that support mobility, and scale to larger user base. With modernization in the cloud applications will deliver capabilities through microservices supporting cybersecurity and cross-functionality with other applications and data analysis services. These benefits improve scalability, fault tolerance, and support agnostic programming languages and technologies. Developing these capabilities will not be limited to a single programming language. Deploying applications will be simpler, more efficient, and reusable across different FDC business areas. These are advantages of the CSP, and funding is critical to this strategy.

Below are comparisons of agency IT budgets as a ratio of total budgets. The Department's IT budget to total budget is below similar agencies. The ratio limits the Department's ability to recover from the negative impacts of existing technical debt.

Table 9: *IT Budget Ratio to Total and IT Staff to Total Staff:*

Agency	IT Budget 23-24	Total Budget 23-24	IT Budget to Total Budget	IT Budget 22-23	Budget Change	IT Positions	Staff	Staff:IT Ratio
Juvenile Justice	8,214,319	678,035,625	1.21%	8,684,126	(469,807)	61	3,246	54:1
Law Enforcement	50,410,232	387,846,654	13.00%	30,433,071	19,977,161	127	1,991	16:1
Children and Families	111,184,237	4,480,973,377	2.48%	88,372,481	22,811,756	233	12,265	53:1
Corrections	59,071,720	3,300,042,237	1.79%	44,240,860	14,830,860	180	23,120	129:1

The table below shows the potential budget to scale with the total FDC budget, using the ratios of state agencies with similar lines of business. Comparisons are with Law Enforcement and Children and Families. The comparisons show the relative increases that result and improves FDC's ability to address issues of technical debt.

Table 10: *FDC IT Budget Scaled to Similar State Agencies*

Agency	Total IT Current Budget FY 23-24	Total FDC Budget FY 23-24	FDC IT Budgets (Scenario) Using Agencies' Rates with Comparable Lines of Business	Rate from Agency
Corrections	59,071,720	3,300,042,237	428,921,825.32	Law Enforcement
Corrections	59,071,720	3,300,042,237	81,882,360.67	Children and Families
Corrections	59,071,720	3,300,042,237	59,071,720.00	Current

4.6 GOVERNMENT DOMAIN

The government domain for the Department is the responsibility for overseeing and managing the state's correctional system. Within the domain there are several services, functions, and operations of FDC including:

Figure 1: *FDC Primary Government Domains*

Protect the public	Manage Institutions and Community Corrections			Rehabilitate Offenders
Incarceration	Rehabilitation	Probation and Parole	Community Corrections	Offender Re-Entry
Security and Safety	Legal and Administrative Processes	Budget and Finance	Staff Training and Development	Data and Reporting

It is important to note that FDC plays a crucial role in maintaining public safety and the proper functioning of the state's correctional system while also striving to rehabilitate offenders.

4.7 SYSTEM USERS

Consistent with the Department's primary domains, system users are distributed across each domain. Business critical functions comprise the majority, but interface with critical systems that support Institutions and Community Corrections.

Table 11: *User Groups of Departmental Systems*

	Application Name	Agency Users
1.	Automated Inmate Ranking System SSIS Database Refresh	Institutions - Classification Management
2.	Comprehensive Inmate Profile Web Interface	Institutions - Classification Management
3.	CPO Caseload	Community Corrections
4.	CSTS (Citizen Services Tracking System)	Institutions – Security Operations
5.	DC Staff Look Up	Institutions – Security Operations
6.	Digital Criminal Scoresheet	Institutions – Security Operations
7.	EAC	Institutions – Security Operations
8.	Emergency Management (EM) - Main application	Institutions – Security Operations
9.	Facility Access Security Tracking (FAST)	Institutional and Community Corrections
10.	Facility Building Management	FMBC
11.	Food Delivery Tracking System (FDTS)	Administration
12.	Gain Time & Disciplinary Reports	Institutions - Classification Management
13.	Health Services Reporting	Health Services
14.	Health Services Utilization Management (HSUM)	Health Services
15.	IG Interdiction	Office of General Counsel
16.	IG Tracker	Office of Inspector General
17.	Inactive HIPAA File Search	Community Corrections
18.	Inappropriate Inmate Behavior	Institutions - Classification Management
19.	Inmate at a Glance	Institutions - Classification & Release Management
20.	Inmate Grievance Logs	Office of General Counsel
21.	Inmate Management Database (IMDB)	Institutions - Classification Management
22.	Inmate Mortalities	Health Services
23.	Inmate Photo Services (Inmate Photo)	Institutions, Community Corrections, Administration
24.	Inmate Photo Services Photo Match	Institutions, Community Corrections, Administration
25.	Inmate Records Tracking System (IRTS)	Central Records
26.	Inmates Face Sheets	Institutions - Classification & Release Management
27.	InMeals (RDP)	Chaplaincy
28.	Lock and Key	Institutions – Security Operations
29.	Mental Health Inmate Transfer (MHIT)	Health Services
30.	Priority Ranking	Institutions - Classification Management
31.	Security Threat Operational Review and Monitoring System (STORMS)	Institutions – Bureau of Intelligence
32.	Self Injury Profiling System (SIPS)	Health Services
33.	Sentence Structure	Institutions – Admissions & Release

	Application Name	Agency Users
34.	Spectrum2	Office of Programs & Re-Entry, Program Development
35.	SVPPU (Sexual Violent Predator Program Utilities)	Institution – Admissions and Release
36.	Update Escapes	Institutions
37.	Volunteer Central Registry	Office of Programs & Re-Entry
38.	WCF_MINS Incidents	Emergency Action Center
39.	Work Release Inmate Monitoring System (WRIMS)	Institutions - Classification Management
40.	Automated Inmate Ranking System (AIRS)	Institutions - Classification Management
41.	CINAS - Corrections Integrated Needs Assessment System	Office of Programs and Re-Entry – Program Development
42.	Classification Appointments Overview and Scheduling System (CAOSS)	FCOR
43.	FCOR - CMS (Super Docket & Victims Notifications Letters)	FCOR
44.	FCOR - CMS (Super Docket & Victims Notifications Letters) Revised App	FCOR
45.	FCOR MACNet	FCOR
46.	FCOR Performane Based Budgeting (PBB)	FCOR
47.	HR - Disaster Overtime Processing System (DOTS)	Human Resources
48.	Inmate Population Counter (IPC)	Institutions – Population Management
49.	Inmate Risk Management System (IRMS)	Office of Institution - Classification Management
50.	Institutional Facilities Tracker (IFTS)	Office of Institutions
51.	Offender Needs Assessment System (ONAS)	Office of Institution - Classification Management
52.	Acknowledgements	FDC
53.	ACTS - Automated Correctional Task System	General Council
54.	ADA Tracking	Institutions
55.	Agency AMS	FDC
56.	Application Security Manager (ASM)	OIT
57.	Arsenal Reports	Office of Institution - Security Operations
58.	CMS - (stands for contract management system - replacement for GS Vendor Tracking)	Office of Institution - Security Operations
59.	CPAS	Office of Institution - Security Operations
60.	Criminal Justice Standards & Training Commission (CJSTC)	Professional Development
61.	Department of Corrections Accreditation Management Systems (DCAMS)	Office of Institution - Security Operations
62.	Digital Disbursement	Finance & Accounting
63.	DOC Custom Error Page	Office of Institution - Security Operations
64.	DOC Event Viewer	Office of Institution - Security Operations
65.	EAS	Office of Human Resource
66.	Employee PIN	Administration
67.	Facility Lookup	FMBC
68.	Family Preparedness	Office of Human Resource
69.	FCOR Agency Details	FCOR Users
70.	FCOR Application Inventory	FCOR Users
71.	FCOR Application Security Manager (ASM)	FCOR Users

	Application Name	Agency Users
72.	FCOR Call Log	FCOR Users
73.	FCOR CLS Application	FCOR Users
74.	FCOR Communication and Legislative Affairs Tracking System (CLATS)	FCOR Users
75.	FCOR Event Viewer	FCOR Users
76.	FCOR Frontend	FCOR Users
77.	FCOR Legacy MACNET (Database only)	FCOR Users
78.	FCOR Legal Tracker	FCOR Users
79.	FCOR Restoration of Civil Rights (CRC) Review Forms	FCOR Users
80.	FCOR Revocation Mail Tracking	FCOR Users
81.	FCOR Staff Directory TEAM DIR	FCOR Users
82.	FCOR Terminated Personnel Files	FCOR Users
83.	FCOR Warrants Tracking	FCOR Users
84.	Human Resources Tracking System (HRTS)	Human Resources (Recruitment)
85.	IG Training and Certification System	Office of General Counsel
86.	Inactive Offender File Error Report	Office of Community Corrections
87.	Inactive Offender File Search	Office of Community Corrections
88.	IT AppInventory	Office of Information Technology
89.	Juvenile Tour Program	Office of Programs & Re-Entry
90.	Offender ISearch (Public)	Public Information Office
91.	Officer Applications	Office of Institution/Health Services/Community Corrections/Programs and Re-Entry
92.	Operational Review/Report Writer (ORRW)	Office of Institution - Security Operations
93.	OSCA Web Service	Office of Information Technology
94.	PASS - Program Attendance Scheduling System	Office of Programs & Re-Entry
95.	Performance Measures Contact Tracking System (PMCTS)	P&P Field Services
96.	Personnel Applicant Tracking System (PATS)	Office of Human Resources
97.	PPRecap	Office of Community Corrections
98.	Promotional IQ	Office of Human Resource
99.	Public Re-Entry Resource Directory	Office of Programs & Re-Entry
100.	Public Web	Public Information Office
101.	Risk and Needs Archive (RANA)	Office of Institution - Classification Management
102.	RecordsTrac	Office of Institution - Classification Management
103.	RESTFulActiveDirectory	Office of Information Technology
104.	Rules Tracking System	Office of General Counsel
105.	Security Access Request (SAR)	Office of Information Technology
106.	SSRC Request	Office of Information Technology
107.	Technical Infrastructure Management System (TIMS)	Office of Information Technology
108.	Volunteer Intake Process (VIP)	Office of Programs & Re-Entry
109.	WCF_ReEntryResourceDirectory	Office of Information Technology

4.8 IMPORTANT INTERFACES

There are over a hundred multiple interfaces across the Department's Applications Portfolio. The primary source of data that supports these critical applications is the Offender Based Information System. Interfaces also include interfaces pertaining to court and legal affairs, financial data, health data, and state records related to mortality and life changes.

	Application Name
1.	Automated Inmate Ranking System SSIS Database Refresh
2.	Comprehensive Inmate Profile Web Interface
3.	CPO Caseload
4.	CSTS (Citizen Services Tracking System)
5.	DC Staff Look Up
6.	Digital Criminal Scoresheet
7.	EAC
8.	Emergency Management (EM) - Main application
9.	Facility Access Security Tracking (FAST)
10.	Facility Building Management
11.	Food Delivery Tracking System (FDTS)
12.	Gain Time & Disciplinary Reports
13.	Health Services Reporting
14.	Health Services Utilization Management (HSUM)
15.	IG Interdiction
16.	IG Tracker
17.	Inactive HIPAA File Search
18.	Inappropriate Inmate Behavior
19.	Inmate at a Glance
20.	Inmate Grievance Logs
21.	Inmate Management Database (IMDB)
22.	Inmate Mortalities
23.	Inmate Photo Services (Inmate Photomatch)
24.	Inmate Photo Services PhotoMatch
25.	Inmate Records Tracking System (IRTS)
26.	Inmates Face Sheets
27.	InMeals (RDP)
28.	Lock and Key
29.	Mental Health Inmate Transfer (MHIT)
30.	Priority Ranking
31.	Security Threat Operational Review and Monitoring System (STORMS)
32.	Self Injury Profiling System (SIPS)
33.	Sentence Structure

	Application Name
34.	Spectrum2
35.	SVPPU (Sexual Violent Predator Program Utilities)
36.	Update Escapes
37.	Volunteer Central Registry
38.	WCF_MINS Incidents
39.	Work Release Inmate Monitoring System (WRIMS)
40.	Automated Inmate Ranking System (AIRS)
41.	CINAS - Corrections Integrated Needs Assessment System
42.	Classification Appointments Overview and Scheduling System (CAOSS)
43.	FCOR - CMS (Super Docket & Victims Notifications Letters)
44.	FCOR - CMS (Super Docket & Victims Notifications Letters) Revised App
45.	FCOR MACNet
46.	FCOR Performane Based Budgeting (PBB)
47.	HR - Disaster Overtime Processing System (DOTS)
48.	Inmate Population Counter (IPC)
49.	Inmate Risk Management System (IRMS)
50.	Institutional Facilities Tracker (IFTS)
51.	Offender Needs Assessment System (ONAS)
52.	Acknowledgements
53.	ACTS - Automated Correctional Task System
54.	ADA Tracking
55.	Agency AMS
56.	Application Security Manager (ASM)
57.	Arsenal Reports
58.	CMS - (stands for contract management system - replacement for GS Vendor Tracking)
59.	CPAS
60.	Criminal Justice Standards & Training Commission (CJSTC)
61.	Department of Corrections Accreditation Management Systems (DCAMS)
62.	Digital Disbursement
63.	DOC Custom Error Page
64.	DOC Event Viewer
65.	EAS
66.	Employee PIN
67.	Facility Lookup
68.	Family Preparedness
69.	FCOR Agency Details

	Application Name
70.	FCOR Application Inventory
71.	FCOR Application Security Manager (ASM)
72.	FCOR Call Log
73.	FCOR CLS Application
74.	FCOR Communication and Legislative Affairs Tracking System (CLATS)
75.	FCOR Event Viewer
76.	FCOR Frontend
77.	FCOR Legacy MACNET (Database only)
78.	FCOR Legal Tracker
79.	FCOR Restoration of Civil Rights (CRC) Review Forms
80.	FCOR Revocation Mail Tracking
81.	FCOR Staff Directory TEAM DIR
82.	FCOR Terminated Personnel Files
83.	FCOR Warrants Tracking
84.	Human Resources Tracking System (HRTS)
85.	IG Training and Certification System
86.	Inactive Offender File Error Report
87.	Inactive Offender File Search
88.	IT AppInventory
89.	Juvenile Tour Program
90.	Offender ISearch (Public)
91.	Officer Applications
92.	Operational Review/Report Writer (ORRW)
93.	OSCA Web Service
94.	PASS - Program Attendance Scheduling System
95.	Performance Measures Contact Tracking System (PMCTS)
96.	Personnel Applicant Tracking System (PATS)
97.	PPRecap
98.	Promotional IQ
99.	Public Re-Entry Resource Directory
100.	Public Web
101.	Risk and Needs Archive (RANA)
102.	RecordsTrac
103.	RESTFulActiveDirectory
104.	Rules Tracking System
105.	Security Access Request (SAR)
106.	SSRC Request
107.	Technical Infrastructure Management System (TIMS)

	Application Name
108.	Volunteer Intake Process (VIP)
109.	WCF_ReEntryResourceDirectory

5 Transition

EOL applications included in this strategy does not include the Offender Based Information System (OBIS). There are 137 applications maintained in the Department's Applications Portfolio that support critical functions. The Cloud Readiness Assessment in Spring 2023 highlighted critical risks for over 70% of these applications, since they leveraged Windows Server 2012, which will be unsupported beginning October 10, 2023. Additionally, these same applications reside on SQL Server 2012 platforms, which were unsupported since July 12, 2022. Consequently, these servers and databases no longer receive security updates, non-security updates, current updates, or technical support.

Adopting the Cloud First Strategy is the Department's response to the essential task of mitigating these risks. This approach enables the Department to upgrade systems with extended support, set respectively for July 2026 and January 2027. However, the Department must remain vigilant to prevent a relapse into the pitfalls of technical debt.

The Department worked internally and consulted with several vendors to perform the readiness assessment to evaluate potential factors involved in migrating to the cloud. Factors to consider in this shift included:

- Funding constraints
- Prioritizing applications that are at end-of-life (EOL); no longer supported by vendors with security patches, and criticality to FDC operations
- Business area availability to participate in project efforts
- Information Security Compliance and protection: Rule 60GG-4.004 F.A.C.
- Compliance with Criminal Justice Information Services (CJIS) Security Policy
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Service Level Agreements (SLAs)
- Required resource skill sets

5.1 Architectural Overview

5.1.1 Data and Reporting Requirements

The department mandates that all applications comply with the continuous data warehousing policy. In line with our modernization initiative, the data warehouse, specifically the Operational Data Store, will serve as the "source of truth" for all reporting and information 'outputs' produced by an application. This necessitates the simultaneous update of both the Online Database and the Data Warehouse for all transactional activities, including Updates, Inserts, and Delete transactions.

For reporting requirements, designers and architects will collaborate with the warehouse team to establish and utilize new or existing Cubes or Data Marts, ensuring the production of the necessary outputs.

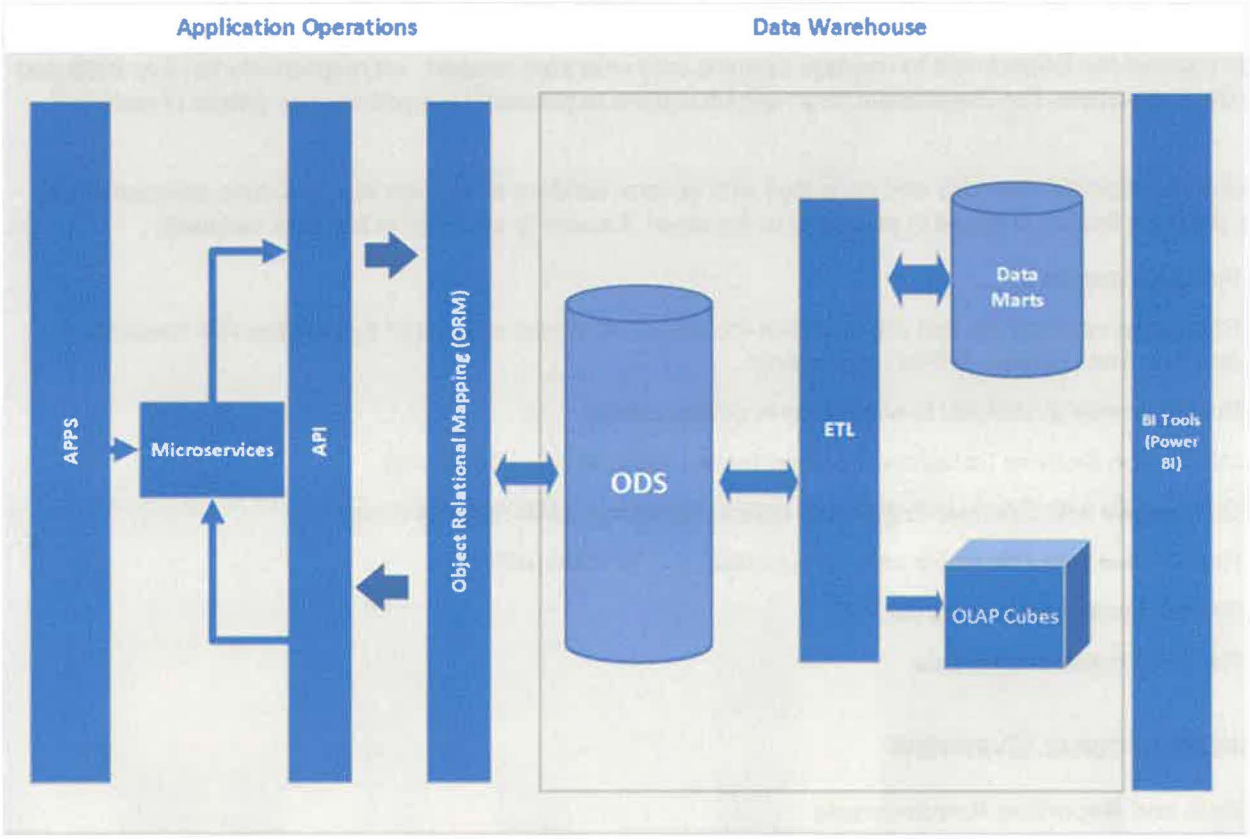
All interactions with the data warehouse, except through data visualization or reports, will occur via the Warehouse API. Architects and Analysts will partner closely with the data team to create the API Façade tailored for the application.

The warehouse operates under a Fetch policy and loading data through Flat files is prohibited. Applications must access required data in the Online Databases (if any) exclusively through the API. Any direct loading of data into the Microservice/Application database(s) is forbidden, except through the Warehouse API via a Fetch mechanism. The warehouse will not push data to any external sources on any type of schedule, the external sources will fetch the required data as needed or on demand.

The support for reporting through the data warehouse implements strict data security and access policies that are consistent with the posture of FDC. Business users will be provided access on a zero-trust basis, therefore, mitigating vulnerabilities and elevation of privileges.

Below is a conceptual EA diagram that provides a Conceptual Microservice solution. It further details the interactions from the API to the Operational Datastore, as well as the ETL processes designed to extract and transfer data to the Reporting cubes and/or data marts for use in Power BI.

Figure 2: *Data Warehouse Support for All Reporting*



5.2 APPROACH

The Department plans to implement a four-phased strategy to modernize applications and restore IT operations and management from technical debt. The process starts with a lift and shift of application and database servers from the State Data Center to the Cloud, re-engineering mission-critical applications that are end-of-life, restoring other business applications that are end-of-life, and planning for a continual refresh of application technology by requesting recurring funds to maintain applications with annual upgrades...

5.2.1 Applications Restoration Strategy

Application restoration is within the technology domain. The four phases of the applications restoration strategy that addresses 137 agency applications are described below.

Figure 3: *4-Phased Modernization Strategy*

- **Phase 1:** Lift and Shift eligible applications.
- **Phase 2:** Re-engineer Mission Critical end-of-life applications.
- **Phase 3:** Modernize applications that are near end of life.
- **Phase 4:** Planning and Funding for Continual Annual Refresh of Application Technology

5.2.2 Phase 1: Lift and Shift

The strategy for Phase 1 is "lift and shift". Lift and shift are process steps to migrate existing applications, databases, servers, and user data. It does not require software coding to migrate the Department's existing applications to Azure quickly. In lift and shift the SQL Server OS, SQL Server Database and code all stay the same. At minimum, any applications with hard-coded links may need some of those links revised to point to correct sources.

5.2.3 Phase 2: Re-Engineer Mission Critical Applications

During phase 2, the Department plans to re-engineer mission critical applications that are at end-of-life. These are a priority as they impact operational business functions across the Department. Areas affected include Inmate support in food, health, and other services.

5.2.4 Phase 3: Modernize Apps Nearing EOL

During phase 3, the Department plans to modernize 137 applications either by rearchitecting or rebuilding. Rearchitecting results in modifying the application code base to scale and optimize it for the cloud. Applications will be made more resilient, highly scalable, independently deployable architecturally, and use Microsoft's PaaS to accelerate the process, scale applications, and improve app management.

A connecting approach during phase 3 is to rebuild applications using cloud-native technologies using the PaaS service model. This will ease expense and complexity with licensing, removing the need for application infrastructure, middleware, or other resources. The Department can then focus on managing the applications and services, without the concern of the servers or databases.

Problem: Over 70% of critical and EOL applications will no longer be supported past October 2023.

- Apps create or use the same data.
- Apps directly access OBIS instead of ancillary data warehouse sources and services.
- There are no data governance practices directing the data life cycle:
    - data creation
    - use
    - sharing / reporting
    - archiving

- destruction.

- The Department is creating waste through accumulating data that is not governed by specific records management and records retention policies and procedures.

Key Outcomes from Phase 3

- A selected vendor will be contracted to rearchitect and rebuild this portfolio of FDC applications.
- Applications will be categorized and architected based on factors such as criticality.

5.2.4.1 Deliverables for Each Application

Consistent with the technology restoration plan and program goals, the application modernization project will include deliverables for each application. The Department's responsibilities require that reliable records be retained for systems, given the requirements of CJIS 5.9.1, the State of Florida Public Records Guide for Law Enforcement Agencies (2021 Edition), and General Records Schedule GS1-SL For State and Local Government Agencies (June 2023).

From the TRP project, the below deliverables will be included:

- Data governance group and processes to oversee orchestrated data life cycle processes in the Department.
- A records management entry including the use of appropriate retention storage media.
- A written records management schedule to move data from online systems to historical storage conforming to the costs to store and retrieve data.
- A data architecture plan for inmate and offender data that includes both OBIS-related data and eSystems data.
- Vendor deliverables for each application will include:
  - Dataflow documentation.
  - Interface documentation.
  - Input / Output documentation.
  - Data dictionary for data involved in the application.
  - Application design.
  - Business processes supported documentation.

5.2.5 Phase 4: Planning and Recurring Funding of Application Technology

The Department cannot revert to the current state of technical debt that has severe impact on its ability to meet its public safety responsibilities across the Department's business domain.

5.3 Staffing and Budget Considerations

The Department performs IT maintenance and operations with a staffing ratio of end users to IT support staff that is about 275% greater than the average for state agencies. This is a significant deficiency for the Department, which makes it difficult to keep applications and databases updated with current technology and compliant with architecture and information security standards. The lack of adequate staffing and spend authority to purchase

new technology must be addressed for the Department to implement a successful Cloud Strategic Plan. The Department plans to request funding at the next Legislative Budget Committee meeting for access to the Cloud Modernization funds and by submitting a Legislative Budget Request for the Fiscal Year 2024-25.

The Department plans to request spending authority over a 3.5-year period, which is attached as **Exhibit A – Budget Detail**.

5.4 Application Considerations

The Department has categorized each of the 137 applications by function to identify which are mission critical and which are non-mission critical business applications. Additionally, the Department has identified the applications that contribute to the total agency technical debt and which applications are currently supported. The restoration strategy blends these two attributes together to classify the applications into three groups that prioritize the need by

Table 12: *Groups of Applications for Restoration*

Groups by Priority	Grouping Criteria	Number of Applications
Group 1	Applications that are categorized as both Mission Critical and end-of-life and contribute to the agency technical debt.	43
Group 2	Other business support applications that are end-of-life and contribute to the agency technical debt.	90
Group 3	The remaining applications, either mission critical or business support only that were not end-of-life during Phases 1 and 2 but are now or soon to be end-of-life. Without recurring funding, these applications will contribute to the agency accumulating additional technical debt.	4

6 Contractual Considerations

The Department continues to evaluate several contracting factors, to support FDC's long-term goals, and to justify engaging Providers. Business areas are involved, as due diligence, to identify their needs and requirements that are key in choosing the vendor. Internally, scoping business areas aligned with the two key divisions of FDC: **Institutions** and **Community Corrections**.

Additional scope areas include assessing the vendor's ability to support regulatory compliance in the cloud and the risks to the Department. Also of importance to the Department is the types of **disaster recovery** (DR) and **outage** scenarios that are consistent with FDC's mission. For DR and outages, SLA measurements will be negotiated for service quality, based on business criticality.

Measurements included are, for example, *recovery time objective* (RTO), *recovery point objective* (RPO), and *maximum allowable downtime* (MAD), which were critical factors to FDC's shift to the Azure Government cloud. Each of these factors is essential to how the Department responds and how the Provider will handle outage and recovery scenarios.

6.1 Roles of Stakeholders

In developing the CSP, stakeholders were analyzed to identify their needs and priorities. For internal stakeholders, two factors were considered 1) influence, 2) interest. After, stakeholder needs were converted into high-level strategic goals. Goals were based on lagging indicators that have accumulated over time that indicate value to stakeholders. As an internal stakeholder group OIT, Institutions, Community Corrections, and administration components were focused on service quality, including DR, cybersecurity, and IT security.

External stakeholders were also identified and included the Governor's Office, Legislators, Northwest Regional Data Center (NWRDC), and the Cloud Services Provider. Similarly, this group of stakeholders was also categorized using the same two factors of influence and interest. The Governor's Office is interested in both service quality factors and funding. Legislators have similar stakeholder focus. NWRDC stakeholder focus was on service usage.

6.2 Performance Monitoring

Performance monitoring is a real-time process that is a component of the cloud-first strategy that is afforded by moving to the new provider. The data available by monitoring tools will help the Department know that the Provider is efficiently apportioning and allocating all resources to fulfill business area demands, consistent with SLAs.

6.3 Exit Strategy

The Department will negotiate a cloud exit strategy as part of contracting with the new provider. The exit strategy affords the Department to avoid vendor lock-in, in the event services, pricing, or capabilities are not responsive to departmental requirements. The Department recognizes that an exit strategy is necessary before going into the selection of a provider and is part of negotiating agreements. Additionally, the Department selected a pay-as-you-go price versus pricing reserved instances. Pay-as-you-go leverages the operating expense model of the cloud that is based on demand versus the term commitment.

6.4 Pricing

The budget detail for implementing the agency Cloud Strategic Plan is attached as **Exhibit A – Budget Detail**.

6.5 SERVICE LEVEL AGREEMENTS

Service Level Agreements are the foundation of ensuring contracted cloud services perform as expected and achieves three key considerations:

- Availability
- Resiliency
- Performance

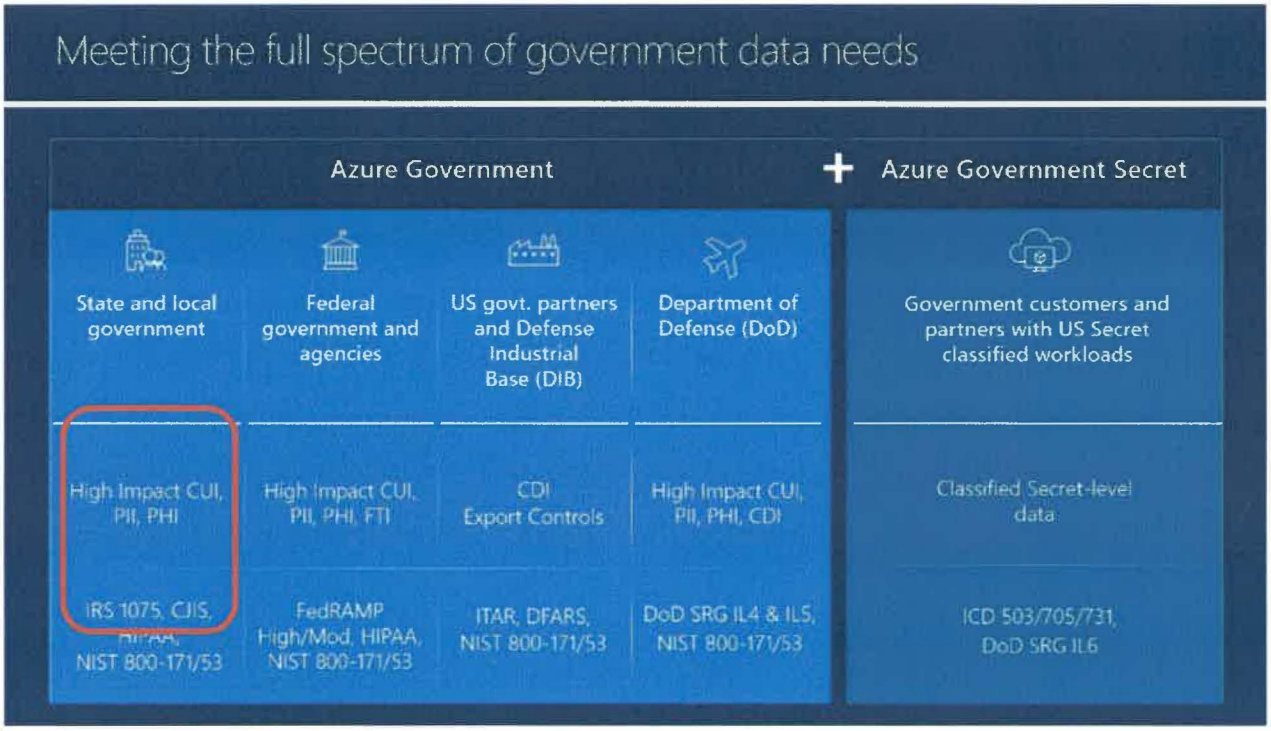
These areas are critical to the quality of departmental business operations, given the nature of FDC's responsibilities that have public safety consequences. Transitioning to the cloud strategy involved these factors as current failures cannot sustain the performance required by FDC.

Availability and performance are closely related, as performance incorporates availability. The cloud service must be resilient, given the natural environment. Consequently, capabilities such as disaster recovery and business continuity that are not currently available are required as parts of the Department's CSP.

7 Security and Risk Planning

The Department's cloud strategy addresses security and risk considerations, embodied in F.S. 60GG-4.004 that are required for state agencies in Florida. Additionally, the Department, as a criminal justice agency is obligated to comply with Criminal Justice Information Services (CJIS) program. Shifting to the Azure Government Cloud affords FDC use of a FedRAMP certified platform that provides higher levels of security for government systems.

Figure 4: *FDC CSP Approach to Managing Security and Risk*



60GG-4.004 incorporates by references compliance with FIPS 199 that provides guidelines and standards for categorizing and classifying information systems based on their impact levels with regard to their CIA:

- Confidentiality
- Integrity
- Availability

FIPS 199 is a critical component of the Risk Management Framework, to assess and manage information and cybersecurity of agencies' information systems. FDC is improving its security posture, to manage the agency's risk profile. Key components of the process supporting the CSP will be implementing the SP 800-30 framework, SP 800-171, 53 for FDC applications.

7.1 Identity and Access Management

Identity and Access Management (IAM) is about the users, processes, and procedures in place to handle the **full** lifecycle of their identities. The CSP incorporates integrating IAM where all users will be given access to system resources, in association with authorized access by their identity. IAM will use Active Directory to manage identities and user authentication for users, groups, and applications. These are high risk cybersecurity components.

Moving to the cloud also provides FDC with options to use a selected IAM solution or the use of the IAM services to support the following such as:

- Multi-factor Authentication (MFA) as a layer of security and account protection for all access to FDC resources, as resources will be in the cloud.
- Role-based Access Control (RBAC) that allows assignment of roles to users, groups, or applications at different levels of Azure resources defining what actions a user performs. RBAC allows greater granularity to specify access to FDC resources.
- Conditional Access Policies that define policies based on conditions such as location, type of device, risk level, while dynamically controlling access.
- Privileged Identity Management (PIM) allows management, control, and monitoring access internally within FDC for temporary access.
- Audit and Monitoring tools to track and review access and changes to resources.
- Service Principals for identities used by applications and services to securely access Azure resources. Also referred to as Service Access provided by microservices.
- Access Reviews to routinely review and update access permissions to ensure alignment with principles of least privileges.

7.2 Data Protection

The Department implements data protection in the cloud across each of the stages of the data lifecycle: Create, Store, Use, Share, Archive, and Destroy. Transport Layer Security (TLS) is the minimum standard supported by the CSP. Encryption upon creation will protect against attack vulnerabilities from hackers or insider threats. Secure key management capabilities are components of the FDC data protection strategy. Data will be encrypted when stored at rest.

Use is complex, however the FDC strategy implements access via API microservices that allow granular application of access and authorization. Operational considerations include use of BYOD, rights, and role management. Data owners responsible for classifying, protecting, and overseeing organizational data use should limit users only to functions absolutely required to perform assigned tasks.

Sharing data will implement data loss prevention (DLP) also described as egress monitoring prevents data from leaving FDC's control. DLP applies to on premise, use of mobile devices, and use in the cloud.

7.3 Disaster Recovery

The FDC CSP acknowledges the significance of disaster recovery (DR) and business continuity (BC) in shifting the cloud-first principles. During application modernization, the Department will conduct a business impact analysis (BIA) for cloud-specific issues to address new risks and opportunities. Multiple connections with the Provider are part of establishing cloud service agreements. Without connectivity, DR and BC activities cannot be performed.

The Azure Cloud offers DR and BC capabilities. Consideration of DR and BC events include responding to Data Breaches or inadvertent disclosure, and vendor lock-in/lock-out. The Department may also consider cloud backup services as part of failover capabilities.

7.4 DATA CONFIDENTIALITY

There are multiple layers to the Department's approach for data confidentiality. The CSP incorporates data governance as essential to successfully comply with state and federal regulations. Each business entity has ownership over its data. OIT, as the custodians tasked with daily administration responsibilities must be provided with the resources of staff and technologies.

Business areas in FDC are data stewards that fully understand the context of data and use this knowledge to determine how each piece of data is used. These are essential points of the Department's data oversight approach, that will be critical during the shift to the cloud. There are four key areas of the data strategy that will be part of the overall CSP.

7.4.1 Four Enabling Data Confidentiality Requirements

Achieving and retaining regulatory compliance begins with understanding how data will be used. Data owners, in each primary business area will be part of the data inventory process that is performed to:

- Categorize all FDC data – required for business functions, controlling business unit, and designating a staff role as the decision maker.
- Classify these data according to overall organizational policies based on the characteristics of specific datasets and assign **sensitivity, jurisdiction,** and **criticality.**
- Classification policies that each business area follows defining roles that can be part of automated data classification systems.
- Data mapping will provide meaning in each area of use, as it moves across the Department, therefore as sensitive data moves across business areas, it retains its *classification* and does not lose its protection.

8 Workload, Capacity, and Connectivity Assessment

Assessment of workload, capacity, and connectivity are critical for the Department to understand the technical landscape, challenges, and dependencies. Defining the legacy environment, provides relevant information to determine requirements in the cloud. These are critical data points that support the Departments cloud migration strategy.

The capacity assessment evaluated application requirements for high-level workloads, which occur at points of average and peak utilization of workloads. Defining current capacity established baseline and future capacity needs. Workload analysis and understanding average and peak workloads are key steps the Department identified to plan cloud infrastructure capacity.

Effectively supporting workloads and capacity required evaluation of network requirements to support workloads in the cloud. Bandwidth was assessed with respect to latency sensitivities for user scenarios, and network features needed by departmental users, such as, virtual private networks (VPN). Assurance that workloads can be processed effectively across the enterprise supports making correct choices in the cloud. An example is the Department's upgrade of the Express Route.

8.1 COMPUTING

Compute resources in the cloud are computing resources that are delivered over the internet. This includes processing power, memory, storage, and networking. Cloud computing providers offer a wide range of compute resources, from small virtual machines to large bare-metal servers.

Compute resources in the cloud are highly scalable and are typically billed on a pay-as-you-go basis. Therefore, the Department will only pay for the resources that are used. This can be a significant cost savings, as there will be no need to make capital investments in and maintain an on-premises IT infrastructure. Compute resources in the cloud can be used to run a wide range of applications, including websites, web applications, databases, and enterprise applications. Some of the additional advantages include:

- **Reliability:** Cloud computing providers offer a high level of reliability, with uptime guarantees of 99.9% or more. This means that the Department can be more confident that its applications will be available when needed.
- **Security:** Cloud computing providers offer a variety of security features to protect data. This includes data encryption, access control, and intrusion detection and prevention systems.

8.2 STORAGE

The provider is responsible for storage in the cloud. Servers and internetworking infrastructures are maintained by the provider who is responsible for hosting, managing, and securing data stored on its infrastructure. The provider ensures that data on its servers is always accessible via public or private internet connections.

Cloud storage offers several advantages over traditional on-premises storage solutions, including:

Accessibility: Cloud storage can be accessed from anywhere with an internet connection, making it ideal for remote workers and mobile users.

- **Scalability:** Cloud storage is highly scalable, meaning that the Department can easily add or remove storage capacity as needed.
- **Cost savings:** Cloud storage can be more cost-effective than on-premises storage, as the Department only pays for the storage used.

- **Security:** Cloud storage providers typically offer a variety of security features to protect data, including encryption, access control, and auditing.

8.3 NETWORK

The Department has installed a 1 gigabit Express Route connection between the State Data Center and the Azure Government Cloud. This circuit is projected to be adequate to meet the Department's needs. Express Route connections are easily and quickly scalable if latency is observed. A similar dedicated connection could similarly be established with other cloud providers as needed.

9 Terms and Definitions

Terms	Definitions
APP-MOD Project	Application Modernization Project for restoring FDC applications
Azure Government Cloud	Azure Government is a Microsoft Government cloud computing service providing dedicated cloud services. It is designed to bring commercial cloud computing capabilities to classified environments. Government agencies can transform mission-critical workloads to the cloud. Notably, it is offered as either of the three cloud service models: • Infrastructure-as-a-Service (IaaS), • Platform-as-a-Service (PaaS), or • Software-as-a-Service (SaaS) Azure Government services can accommodate data that is subject to various government regulations and requirements.
6-Rs	The 6 Rs of cloud migration—re-host, re-platform, repurchase, retain, retire, and re-factor—can help to determine clear paths for migration.
CIO	Chief Information Officer
Critical to Quality	**CTQ:** Measurable performance characteristics of a process, product, or service that are critically important to customers.
EOL	End-of-Life
FDC or Department	Florida Department of Corrections
Leadership	FDC Executive Leaders
Lift-and-shift	A migration strategy that is a path of least resistance that re-hosts existing workloads without modifications of applications or redesign of how they are hosted.
OCC	Office of Community Corrections
OIT	Office of Information Technology
PMO	Portfolio management office
SIO	Security and Institutions Office
SIPOC	An effective method for stakeholder identification, analysis, and communication. SIPOC – Suppliers, Inputs, Processes, Outputs, Customers.

Terms	Definitions
	It is visually mapping processes and stakeholder needs with: • project scope, goals, stakeholder requirements, and • establishing alignment across leadership and project teams. SIPOC is critical for improving processes, methods, or functions as it searches out for stakeholders involved or affected and eliminates those that are not involved or affected. Lean principle for stakeholder analysis and effective communications related to and supporting organizational change management (OCM).
SME	Subject matter expert
SOP	Standard operating procedure
Stakeholder	PMI defines stakeholder as individual, group, or organization affected by or may be affected by project decisions, activities, or outcomes. Lean amplifies the definition as: stakeholder being invested in the process and impacts how well the process performs (See SIPOC). • Stakeholders are everywhere. • Not just operators • Involved in one or more activities in a process. **Lean** amplifies the definition as: stakeholder being invested in the process and impacts how well the process performs.
Technical debt	Technical debt is the term applied to a cycle of avoided costs that over time causes ongoing business and operational impact. It transfers technical risks from this debt to business operations that elevates operational risks.
TRP	Technology Restoration Program.

10 List of Applications

The table lists the Department's Applications Portfolio, criticality, cloud readiness, and cloud strategy. The Department will prioritize applications in alignment with the Budget Plan in Appendix A.

	Application Name	Business Purpose	Criticality Level	Cloud Readiness	Cloud Strategy
1.	Automated Inmate Ranking System SSIS Database Refresh	SQL server integration services tool for AIRS data load.	Business Critical	Lift and Shift	Modernize
2.	Comprehensive Inmate Profile Web Interface	Comprehensive Inmate Profile Web Interface	Business Critical	Lift and Shift	Modernize
3.	CPO Caseload	A web interface for Probation Officers to manage offender visits.	Business Critical	Lift and Shift	Modernize
4.	CSTS (Citizen Services Tracking System)	Correspondence log for citizen services / legislative affairs	Business Critical	Lift and Shift	Modernize
5.	DC Staff Look Up	FDC staff look up application developed to allow users to search resources to retrieve data about staff	Business Critical	Lift and Shift	Modernize
6.	Digital Criminal Scoresheet	Legislative mandate; used by the courts for sentencing guidelines to the judge.	Mission Critical	Lift and Shift	Modernize
7.	EAC	Combines the Use of Force, PREA, and reportable incidents for tracking.	Business Critical	Lift and Shift	Modernize
8.	Emergency Management (EM) - Main application	Management and tracking of operations during emergency activation.	Business Critical	Lift and Shift	Modernize
9.	Facility Access Security Tracking (FAST)	Tracks the entrance and exit of Inmate visitors and institutional volunteers.	Business Critical	Lift and Shift	Modernize
10.	Facility Building Management	This application is the interface for a database that stores images and blueprints of FDC / DMS owned facilities; data is consumed by other applications	Business Critical	Lift and Shift	Modernize
11.	Food Delivery Tracking System (FDTS)	Food Delivery Tracking System	Business Critical	Lift and Shift	Modernize
12.	Gain Time & Disciplinary Reports	Provides data for sentence calculation to account for reducing or extending an inmate's release date. Loss could result in early release.	Mission Critical	Lift and Shift	Modernize
13.	Health Services Reporting	Allows users in the field to enter HIPAA, TB, Risk Management and QM reports electronically	Mission Critical	Lift and Shift	Modernize
14.	Health Services Utilization Management (HSUM)	Health Services Utilization Management is a tool for Health services to look up past and current Inmate referrals for approval	Mission Critical	Lift and Shift	Modernize
15.	IG Interdiction	Tracks k-9 and Interdiction contraband	Business Critical	Lift and Shift	Modernize
16.	IG Tracker	Inspector General tracking system	Business Critical	Lift and Shift	Modernize
17.	Inactive HIPAA File Search	This is the search tool for looking up archived inactive HIPAA files for community corrections	Mission Critical	Lift and Shift	Modernize
18.	Inappropriate Inmate Behavior	Allows staff a simple way to report incidents	Business Critical	Lift and Shift	Modernize
19.	Inmate at a Glance	Provides officers with a comprehensive listing of information about a specific Inmate	Mission Critical	Lift and Shift	Modernize
20.	Inmate Grievance Logs	Inmate Grievance Logs	Mission Critical	Lift and Shift	Modernize

	Application Name	Business Purpose	Criticality Level	Cloud Readiness	Cloud Strategy
21.	Inmate Management Database (IMDB)	Daily inmate callout system; for inmate movement including court dates, religious events, education, medical appointments, and work release.	Business Critical	Lift and Shift	Modernize
22.	Inmate Mortalities	Tracks/Reports inmate deaths	Mission Critical	Lift and Shift	Modernize
23.	Inmate Photo Services (Inmate Photomatch)	Part of the system for synchronizing data that produces a sex offender list with pictures used by FDLE.	Mission Core	Lift and Shift	Modernize
24.	Inmate Photo Services PhotoMatch	Part of the system for synchronizing data that produces a sex offender list with pictures used by FDLE.	Mission Core	Lift and Shift	Modernize
25.	Inmate Records Tracking System (IRTS)	Inmate record tracking system	Mission Core	Lift and Shift	Modernize
26.	Inmates Face Sheets	Produces inmate face sheets with photo and demographic information that can be printed; used by officers for identification and validation of inmate during movement.	Mission Core	Lift and Shift	Modernize
27.	InMeals (RDP)	InMeals - RDP Religious Dietary Program	Business Critical	Lift and Shift	Modernize
28.	Lock and Key	Allows institutions to keep track of individuals that are assigned keys	Mission Critical	Lift and Shift	Modernize
29.	Mental Health Inmate Transfer (MHIT)	Mental health inmate transfer bed tracking system	Mission Critical	Lift and Shift	Modernize
30.	Priority Ranking	Developed to give classification staff ranking information from a weekly extract from the mainframe	Business Critical	Lift and Shift	Modernize
31.	Security Threat Operational Review and Monitoring System (STORMS)	Tracks Gang Information; reported to county SOs for release dates.	Business Critical	Lift and Shift	Modernize
32.	Self Injury Profiling System (SIPS)	Health Services inmate self injury profiling system	Business Critical	Lift and Shift	Modernize
33.	Sentence Structure	The application logs the receipt and processing of court/legal documents, correspondence (received by mail, e-mail or fax) and phone calls affecting and/or regarding calculating the inmates' sentences that are received by the Bureau of Admission and Release	Mission Critical	Lift and Shift	Modernize
34.	Spectrum2	Inmate/Offender Assessment that includes Web Self Assessment	Mission Critical	Lift and Shift	Modernize
35.	SVPPU (Sexual Violent Predator Program Utilities)	Used for tracking violent sexual predators. Critical for medical callouts.	Mission Critical	Lift and Shift	Modernize
36.	Update Escapes	A web interface used by the Emergency Action Center to update status distribute information when an inmate escape is reported.	Mission Critical	Lift and Shift	Modernize
37.	Volunteer Central Registry	This is the internal web application that is part of the volunteer intake process.	Business Critical	Lift and Shift	Modernize
38.	WCF_MINS Incidents	Pulls information from OBIS for reportable incidents, especially PREA incidents; the PREA # is distributed to the EAC for accountability.	Mission Critical	Lift and Shift	Modernize
39.	Work Release Inmate Monitoring System (WRIMS)	Manages Inmates at Work Release Centers; tracks employment, money earned, and program plan progress. Critical for tracking offender movement including entry and exit at facilities.	Mission Critical	Lift and Shift	Modernize
40.	Automated Inmate Ranking System (AIRS)	Ranking component for the Risk and needs replacement	Mission Critical	Lift and Shift	Modernize
41.	CINAS - Corrections Integrated Needs Assessment System	The Corrections Integrated Needs Assessment System (CINAS) ensures the maximum continuity possible from an offender's transition	Mission Critical	Lift and Shift	Modernize

	Application Name	Business Purpose	Criticality Level	Cloud Readiness	Cloud Strategy
		from community supervision to prison and the inmate's re-entry to society. CINAS integrates information, needs and the Community Corrections Recidivism Index Score (CCRIS) collected during an offender's term of supervision into a collective system that measures an inmate's Institutional Inmate Recidivism Index Score (IIRIS) by way of static and dynamic factors and assists the classification team in determining inmate needs.			
42.	Classification Appointments Overview and Scheduling System (CAOSS)	Classification Appointments Overview and Scheduling System	Business Critical	Lift and Shift	Modernize
43.	FCOR - CMS (Super Docket & Victims Notifications Letters)	Commission Management System - case document tracking	Business Critical	Lift and Shift	Modernize
44.	FCOR - CMS (Super Docket & Victims Notifications Letters) Revised App	Commission Management System - case document tracking	Business Critical	Lift and Shift	Modernize
45.	FCOR MACNet	FCOR and Gov. Office application to track RCR applicants	Business Critical	Lift and Shift	Modernize
46.	FCOR Performance Based Budgeting (PBB)	Performance Based Budgeting System, where staff enters time broken down by hours spent on specific tasks and subtasks for audit and reporting purposes	Business Critical	Lift and Shift	Modernize
47.	HR - Disaster Overtime Processing System (DOTS)	This web-based application facilitates HR staff process and report on pay and overtime for staff on disaster codes for federal reporting	Business Critical	Lift and Shift	Modernize
48.	Inmate Population Counter (IPC)	Inmate Population Counter	Mission Critical	Lift and Shift	Modernize
49.	Inmate Risk Management System (IRMS)	Serves as the risk component in the replacement of the old Risk and Needs (RANA) System that is in OBIS	Mission Critical	Lift and Shift	Modernize
50.	Institutional Facilities Tracker (IFTS)	This application tracks various types of incidents in institutions and provides statistics for monthly review	Mission Critical	Lift and Shift	Modernize
51.	Offender Needs Assessment System (ONAS)	Offender needs assessments	Mission Critical	Lift and Shift	Modernize
52.	Acknowledgements	Employee acknowledgements to verify and track staff confirmation of having been provided and read current version of employee handbook	Business Critical	Lift and Shift	Modernize
53.	ACTS - Automated Correctional Task System	This is where charge codes and sentencing information is entered and edited or viewed, tracking statutory changes and sentencing guidelines	Business Critical	Lift and Shift	Modernize
54.	ADA Tracking	Tracks ADA request from Inmates, staff and/or other personnel	Business Critical	Lift and Shift	Modernize
55.	Agency AMS	Account Management System for external agencies. This is the administrative interface for a standardized security system we use for CJNet and external Applications	Business Critical	Lift and Shift	Modernize
56.	Application Security Manager (ASM)	Application Security Manager	Business Critical	Lift and Shift	Modernize
57.	Arsenal Reports	Queries Arsenal Access databases over network file shares for each institution to produce reports from the Access data	Business Critical	Lift and Shift	Modernize
58.	CMS - (stands for contract management system - replacement for GS Vendor Tracking)	Provides the ability to add and track all Department contracts and agreements	Business Critical	Lift and Shift	Modernize
59.	CPAS	Cell phone accounting system where staff who are issued state cell	Business Critical	Lift and Shift	Modernize

	Application Name	Business Purpose	Criticality Level	Cloud Readiness	Cloud Strategy
		phones view and attest to their respective invoices			
60.	Criminal Justice Standards & Training Commission (CJSTC)	Provides academy administrators and coordinators with the ability to generate examinations for use in basic recruit, advanced, and specialized training courses	Business Critical	Lift and Shift	Modernize
61.	Department of Corrections Accreditation Management Systems (DCAMS)	Allows the users to manage their institutions' accreditation files	Business Critical	Lift and Shift	Modernize
62.	Digital Disbursement	Public facing application where victims sign up for direct deposit or other forms of digital payments of COPS funds	Mission Critical	Lift and Shift	Modernize
63.	DOC Custom Error Page	This is a component of the DOC Event Viewer below. The Custom Error Page is called by other applications to show end-users an application error ID they can provide to the helpdesk	Business Critical	Lift and Shift	Modernize
64.	DOC Event Viewer	Allows the Help Desk with trouble shooting uses and console to search errors logged by the DOC Event Logger Utility	Business Critical	Lift and Shift	Modernize
65.	EAS	Emergency Alert System	Business Critical	Lift and Shift	Modernize
66.	Employee PIN	This generates and stores PIN codes for staff that are used in one or more mobile web applications	Business Core	Lift and Shift	Modernize
67.	Facility Lookup	This is the facility search on DCWeb	Business Critical	Lift and Shift	Modernize
68.	Family Preparedness	Used to designate essential personnel in emergency situations as well as acknowledging that a plan is in place for families	Mission Critical	Lift and Shift	Modernize
69.	FCOR Agency Details	Form maintenance tool that addresses changes to the FCOR environment	Business Critical	Lift and Shift	Modernize
70.	FCOR Application Inventory	Application provides a way to track FCOR applications and system tools used by FDC OIT	Business Critical	Lift and Shift	Modernize
71.	FCOR Application Security Manager (ASM)	Manage permissions for FCOR web applications	Business Critical	Lift and Shift	Modernize
72.	FCOR Call Log	FCOR app that tracks calls for Legal	Mission Critical	Lift and Shift	Modernize
73.	FCOR CLS Application	This is a desktop app connecting to legacy databases	Business Critical	Lift and Shift	Modernize
74.	FCOR Communication and Legislative Affairs Tracking System (CLATS)	FCOR App that tracks all request and responses made to and from the Communications and Legislative offices	Mission Critical	Lift and Shift	Modernize
75.	FCOR Event Viewer	Stores Error events from applications for support purposes	Business Critical	Lift and Shift	Modernize
76.	FCOR Frontend	This is a legacy desktop EXE used for manually manipulating the legacy "fpcdb" database, which contains FCOR's legacy HR data. Upon completion of new PBB, there should be nothing using this database with the possible exceptions of legacy MACNET and CLS application if that is still used. Those databases must be eliminated or refactored, so this should not be needed going forward but again this requires follow-up with FCOR to verify any remaining function or needs from the [fpcdb] database.	Business Critical	Lift and Shift	Modernize
77.	FCOR Legacy MACNET (Database only)	Legacy MACNET application - used for historical data research. This needs to be evaluated for compatibility with SQL / OS upgrades and may need a project to transfer or convert old data if it is still needed.	Business Critical	Lift and Shift	Modernize

	Application Name	Business Purpose	Criticality Level	Cloud Readiness	Cloud Strategy
		The app was already replaced with all new architecture			
78.	FCOR Legal Tracker	Legal matters tracker - FCOR Legal	Mission Critical	Lift and Shift	Modernize
79.	FCOR Restoration of Civil Rights (CRC) Review Forms	Clemency restoration of civil rights (RCR)	Business Critical	Lift and Shift	Modernize
80.	FCOR Revocation Mail Tracking	Revocation Process mail tracking	Business Core	Lift and Shift	Modernize
81.	FCOR Staff Directory TEAM DIR	FCOR Staff Directory	Business Critical	Lift and Shift	Modernize
82.	FCOR Terminated Personnel Files	Database for the Terminated Personnel Files, provides HR staff with the ability to store, access, and retrieve personnel files	Business Critical	Lift and Shift	Modernize
83.	FCOR Warrants Tracking	Revocation and arrest warrant tracking for conditional release offenders	Mission Critical	Lift and Shift	Modernize
84.	Human Resources Tracking System (HRTS)	Human Resources Tracking System (HRTS)	Business Critical	Lift and Shift	Modernize
85.	IG Training and Certification System	IG Training and Certification System	Business Critical	Lift and Shift	Modernize
86.	Inactive Offender File Error Report	Inactive Offender Files	Business Critical	Lift and Shift	Modernize
87.	Inactive Offender File Search	Calls an RSS feed populated by MS Search Server to return links to archived offender files on distributed network of file and print servers throughout the state	Business Critical	Lift and Shift	Modernize
88.	IT App Inventory	This is used primarily by the helpdesk to monitor site connectivity statuses throughout the state	Business Critical	Lift and Shift	Modernize
89.	Juvenile Tour Program	Used for scheduling juvenile tours of correctional facilities	Business Critical	Lift and Shift	Modernize
90.	Offender ISearch (Public)	Inmate/Offender information Search (Public) is the public websites	Business Critical	Lift and Shift	Modernize
91.	Officer Applications	Digitized DC forms for mobile devices, currently just includes housing log form but enhancements are in progress	Business Critical	Lift and Shift	Modernize
92.	Operational Review/Report Writer (ORRW)	Web Application used by Internal Audit	Business Critical	Lift and Shift	Modernize
93.	OSCA Web Service	Developed so that the Departments' Inmate/Offender data can be shared throughout numerous state Law Enforcement Agencies in a Collective Initiative for Information sharing	Business Critical	Lift and Shift	Modernize
94.	PASS - Program Attendance Scheduling System	This is for scheduling and tracking inmate participation in programs (i.e., programs and re-entry)	Business Critical	Lift and Shift	Modernize
95.	Performance Measures Contact Tracking System (PMCTS)	PMCTS - Performance Measures Contact Tracking System	Business Critical	Lift and Shift	Modernize
96.	Personnel Applicant Tracking System (PATS)	Tracks the recruitment process for new employees	Business Critical	Lift and Shift	Modernize
97.	PPRecap	This is a reporting system used by Community Corrections using files uploaded from SAS reports as inputs	Business Critical	Lift and Shift	Modernize
98.	Promotional IQ	Generates Questionnaires for specific job codes for interviews	Business Critical	Lift and Shift	Modernize
99.	Public Re-Entry Resource Directory	Application to search and display re-entry resources on the public website	Business Critical	Lift and Shift	Modernize

	Application Name	Business Purpose	Criticality Level	Cloud Readiness	Cloud Strategy
100.	Public Web	Public Website	Business Critical	Lift and Shift	Modernize
101.	Risk and Needs Archive (RANA)	Risk and Needs Assessment	Business Critical	Lift and Shift	Modernize
102.	RecordsTrac	Tracks public and non-public record requests to Central Records	Business Critical	Lift and Shift	Modernize
103.	RESTFul Active Directory	RESTful web service that queries AD/LDAP in real time for individual users. Consumed by other applications (DC Staff Lookup for example)	Business Critical	Lift and Shift	Modernize
104.	Rules Tracking System	RTS - Rules Tracking System	Business Critical	Lift and Shift	Modernize
105.	Security Access Request (SAR)	Application for IT security requests	Mission Critical	Lift and Shift	Modernize
106.	SSRC Request	Simple form for OIT staff to send issues to FDC helpdesk for issues that require data center tickets to be submitted	Business Critical	Lift and Shift	Modernize
107.	Technical Infrastructure Management System (TIMS)	Technical Infrastructure Management System	Business Critical	Lift and Shift	Modernize
108.	Volunteer Intake Process (VIP)	This application automates currently paper based Volunteer intake process starting from volunteer recruitment through final approval for working in institutions	Mission Critical	Lift and Shift	Modernize
109.	WCF_ReEntryResourceDirectory	WCF listener web service; consumed by mainframe to push data to MSSQL databases related to registered re-entry service providers	Business Critical	Lift and Shift	Modernize

11 Exhibit A – Budget Detail

11.1 Technology Refresh Plan for Applications

The Department provides the below budget detail plan that covers the phases of the technology refresh plan for applications. The plan begins with LBC funding for FY23-24. Recurring funding for ensuing phases follows for FY24-25, FY25-26, and FY26-27. The total budget schedule for the four years, including LBC funding FY23-24is $110.3 million.

Table 13: *Technology Refresh Budget Plan*

	2023/24 LBC	2024/25 Phase 1	2025/26 Phase 2	2026/27 Phase 3	Grand Total
Contracted Services	**$17,500,000**	**$17,500,000**	**$30,038,750**	**$45,267,000**	**$110,305,749**
Project Management and Business Analysis	**$5,547,675**	**$9,542,000**	**$19,084,000**	**$19,084,000**	**$53,257,675**
Contracted Services (NR)	$5,547,675	$9,542,000			$15,089,675
Contracted Services (R)			$19,084,000	$19,084,000	$38,168,000
Software Development Services	**$11,952,325**	**$7,958,000**	**$10,954,750**	**$26,183,000**	**$57,048,074**
Non-recurring	$11,952,325	$7,958,000	$1,680,750	$6,909,750	$28,500,824
2023/24 App Restoration (NR)	$11,952,325				$11,952,325
2024/25 App Restoration (NR)		$7,958,000			$7,958,000
2025/26 App Restoration (NR)			$1,680,750		$1,680,750
2026/27 App Restoration (NR)				$6,909,750	$6,909,750
Recurring			$9,274,000	$19,273,250	$28,547,250
2023/24 App Restoration (R)			$5,810,375	$5,810,375	$11,620,750
2024/25 App Restoration (R)			$1,031,375	$1,031,375	$2,062,750
2025/26 App Restoration (R)			$2,432,250	$2,432,250	$4,864,500
2026/27 App Restoration (R)				$9,999,250	$9,999,250
Grand Total	**$17,500,000**	**$17,500,000**	**$30,038,750**	**$45,267,000**	**$110,305,749**