CITY OF KIRKLAND
Information Technology Department
123 Fifth Ave, Kirkland, WA 98033 · 425.587.3050
www.kirklandwa.gov

MEMORANDUM

To: Kurt Triplett, City Manager

From: Smitha Krishnan, IT Director
Xiaoning Jiang, IT Deputy Director

Date: 9/03/2020

Subject: IT Stabilization Implementation Update #3

RECOMMENDATION

It is recommended that the City Council receive a third quarterly update in 2020 on the Information Technology (IT) Stabilization Project, which has been in implementation since September 2019.

BACKGROUND DISCUSSION

In the June 2020 update to City Council, the IT Department provided an overview of the key areas of focus for IT Stabilization:

1. IT Service Management (ITSM) Solution
2. Risk Mitigation Activities
3. IT Security Strategy and Roadmap

An update on the status of IT's capital and operating budget was also provided, with a plan to manage the increased cost of operating in the Microsoft Azure Government Cloud. This memo provides an update on activities completed in the above areas since the last Council update. Additionally, this memo provides recommendations for City Council's consideration regarding alternatives to the Texas Backup strategy for our environment in the Microsoft Azure Cloud.

IT Activities to support the COVID-19 Pandemic

The increased focus on IT Stability is best reflected by a Key Performance Indicator (KPI) for IT Operations. This measure is the number of **Major** and **Priority 1** incidents per month. The table below records the number of Major and Priority 1 incidents for the past six months.

2020 Month	Major Incidents[1]	Priority 1 Incidents[2]	Total[3]
March	0	3	3
April	0	2	2
May	0	2	2
June	0	2	2
July	0	0	0
August	1	0	1

1. A **Major Incident** impacts multiple systems and has a large organizational impact. E.g. Network Down.
2. A **Priority 1** Incident impacts a mission-critical system with multiple users and no workaround available.
3. As reference, the City of Bellevue's monthly target for this metric is ≤ 5 per month.

We experienced an outage of services hosted in Microsoft Azure (available to public) on August 18th. Although there was no impact to technology services internally to City staff, we categorized this as a Major Incident due to the external visibility. Careful investigation was completed with Microsoft and the issue was determined to be outside the City's network. The issue was with the commercial internet provider between Washington and Arizona. In other words, we confirmed that this outage was not related to services provided by either Microsoft or the City.

Below are highlights of IT accomplishments since the last Council Update:

1. Implemented Microsoft Azure's "reserved instance" feature for virtual machines in May. This is a 3-year commitment with Microsoft providing a discount of $12,000 per month.
2. Enabled audio/video capability for the public to engage in Council meetings. Also supported City Leadership and Council in their hosting of a successful virtual 4th of July parade.
3. Supporting the Kirkland Municipal Court (KMC) in implementing OCourt, a SaaS solution to assist the KMC with conducting virtual hearings successfully. This web-based solution will greatly reduce the manual effort for KMC staff to populate, route, and manage the daily case load. This solution is planned to go-live in October.
4. As part of the Desktop Replacement Project this year, IT is working with departments to replace desktops with laptops to continue supporting remote staff during the pandemic.
5. Supported the EOC to fast track the purchase of a tool (JobSiteCheck) to allow City staff and visitors to conduct daily COVID self-assessments before entering City facilities in a highly efficient, protected, time conscious manner.
6. Completed a successful pilot implementation of Microsoft Teams for phone queues for Utility Billing.
7. Implementing a new method (GlobalProtect) for secure remote connections from laptops in September. This solution will further improve security for users connected remotely to the City's network. IT is also using this opportunity to engrain industry best practices to enhance security such as minimizing the use of personal devices for City work.
8. Upgrading the City's phone system in September, which will add increased mobility enabling staff to access their desk phone from anywhere on any device.
9. Launched a new solution for Fleet and Storm Water management replacing two legacy systems that were past their useful life cycle.

Update on Stabilization Implementation Phase 1 Scope of Work

1. **IT Service Management (ITSM) Solution**

   After conducting a thorough review of the previously selected vendor, ManageEngine, IT decided not to pursue this product. There were multiple reasons for this decision, but the primary factor was a disagreement between the legal entities on contract language pertaining to financial liability for the City. Due to the increased risk for the City, this product was not pursued further.

   The team, led by IT Deputy Director Xiaoning Jiang, swiftly shifted gears to publish a new Request for Proposals (RFP) for a comprehensive tool for IT Service Management (ITSM) and IT Asset Management (ITAM). The process was successfully completed, and a new vendor, SummitAI, was selected. The contract is in the final stages of execution with a kick-off planned in September.

   As previously presented to Council, the scope for this implementation includes deploying the modules for:
   a. Incident Management
   b. Service Request Management

c. User Knowledge Base and User-Friendly Customer Portal
d. Change Management
e. Asset Management
f. Configuration Management

The implementation also includes the development of service level agreements tied to these modules, templates, automated workflows, Standard Operating Procedures (SOPs) and training of IT Staff. Attachment A includes a high-level project implementation approach and timeline. This phase is planned to be completed by the end of February 2021, with the customer facing components being launched by the end of this year.

Phase 2 of IT Stabilization project will focus on implementing a solution for IT Operations Management (ITOM). This encompasses purchasing and deploying a consolidated solution to manage the provisioning, capacity, and performance of the City's network as well as applications and systems. Currently, the IT Department has multiple tools that perform monitoring. However, these tools are not being used effectively by staff to be proactive versus reactive in monitoring day-to-day operations. Additionally, managing multiple, disparate tools is an increased burden on staff. The City Manager is evaluating a Service Package to replace the existing tools with a single, consolidated, monitoring solution to shift towards proactive monitoring of the City's infrastructure, applications, systems and data, with performance indicators as part of the 2021-2022 budget process.

2. **Risk Mitigation Activities**

The following projects on the IT Work Plan for 2020, led by Chuck Saunders, IT Supervisor for Network Operations, further advance the department's goals for stability:

1. On-Premise Storage Replacement: This project was completed ahead of schedule and included updating and configuring the remaining storage components on-premise. Completing this project as planned yielded the following benefits for the City:
    - No longer renting space at the City of Bellevue data center (a cost saving)
    - Increased redundancy between City Hall and KJC. This allows us to recover swiftly if one of the locations experiences a large-scale hardware failure
    - Improved performance of storage components

2. Network Infrastructure Replacement: This project includes the replacement of all switches, routers, firewalls and wireless access points. The scope of this project was expanded to include the Kirkland Justice Center in 2020 versus 2021. This project is delayed due to vacancies in the Network team that are currently being filled and is now scheduled for completion in January 2021. From a stability standpoint, this project will yield the following benefits:
    - New equipment appropriately sized to meet the growing needs of the City including supporting a remote workforce
    - Updated network design that adds segregation within the network to reduce the risk of network issues in one building propagating to another
    - New Firewalls that add critical security enhancements for our largely remote workforce during the pandemic, such as:
        a. Integrated URL Filtering, Intrusion Prevention and Reporting
        b. Secure, Unified, Remote Access
            i. Will provide a single client for all devices (personal or City owned)
            ii. Ease of use and support
            iii. Replaces our current model of two different technologies
    - Improves wireless connectivity by eliminating several bottlenecks
    - Reduces the ongoing cost with payment of a 5-year subscription upfront

3. **Security Strategy**

IT engaged CI Security to develop an Information Security Management Strategy and Roadmap for the City. This effort was led by Donna Gaw, IT Manager for Security and Service Management. Donna's role was recently modified to ensure an increased focus on the City's Security Program. The scope of this engagement includes:

1. Review and analyze the security policies and practices of the IT Department.
2. Measure the City's cybersecurity maturity level based on the industry standard for security (National Institute of Standards and Technology Cybersecurity Framework – NIST CSF)
3. Provide a framework for information security governance as well as a tactical roadmap to resolve deficiencies in 6 months, 2021 and ongoing
4. An incident management plan and policy
5. Five playbooks to respond to most likely cyber incident scenarios
6. Set of tabletop exercises to improve incident response readiness among staff and practice using the playbooks.

CI Security concluded that the City of Kirkland's overall security practices are adequate and effective. Tactical security issues are handled well, and the City's compliance posture is not in danger of regulatory action. The biggest deficiency, as expected, is in the documentation of these procedures and knowledge as written policy and playbooks. The current engagement will help identify actions items for the next 18 months to close this gap. Additionally, the roadmap recommends a series of activities that should be performed at the recommended cadence (weekly, monthly, quarterly and annually) to be included in the department's annual work plan. Collectively, these activities will establish automated and repeatable processes (that are no longer dependent on the "tribal knowledge" of individuals) and advance the City's security standing to the desired maturity level.

Key recommendations made by CI Security include:

1. Implement tactical quick wins identified by CI Security in the next 6 months.
2. Prioritize a roadmap of corrective actions identified from this engagement as part of IT's 2021 and ongoing work plans. The following key actions/deliverables will advance the City's security standing to the desired maturity level within 18 months:
    a. Develop a Business Continuity and Disaster Recovery plan with a key focus on security.
    b. Formalize security monitoring of the network and alerting to improve situational awareness and reduce cyber risk
    c. Update IT Policies to account for the "new normal" that has risen in the wake of the pandemic
    d. Assign internal resources for the ongoing oversight and management of the City's Security Program (0.5 FTE) as well as the execution of the security tasks included in the IT Work Plan annually (0.5 FTE). This is being achieved by re-prioritization of existing IT staff priorities to focus on this track.
    e. Create a cross-departmental security governance committee to keep the City's Leadership informed of security risks. This may be the existing IT Steering Team.

Update on Azure Back Up Strategy

In the budget update provided to Council in June, factors contributing to the increased Cloud expenditures were described in detail. One of these factors was the secondary back of Microsoft's Azure Environment to Texas, which was not part of the original scope. Attachment B presents a visual of the City's current backup approach with a secondary backup of the Microsoft Azure environment to Texas at an annual cost of $102,000. This cost will increase annually with the growth of our infrastructure, systems and data and is currently projected to be $564,000 for 5 years. With this backup, the data

stored in Texas is not readily usable in an emergency. It will require standing up significant resources (staff time plus professional services) and anywhere from 2-4 weeks to be usable. One of the biggest constraints with this strategy is the lack of access to the Texas environment outside of an emergency for planning and training. Council concurred with staff concerns regarding this approach and authorized IT staff to evaluate alternatives to the Texas backup.

IT explored a range of options from having no secondary backup to Microsoft's Azure environment in Arizona (least expensive) to a complete hot site in the Government Cloud (most expensive and in the range of $8-11 million). Attachment C presents a visual of the recommended option, which is a secondary backup at the Kirkland Justice Center (KJC) at a 5-year total cost of $246,000. Pros of this option are:

- Significantly less expensive over a 5-year period
- Leverages the City's existing infrastructure
- Readily available to IT staff for testing and training
- Greatly speeds up the time to recover from the secondary backup with more control of what is restored and when.
- No professional services required to configure, test and implement

Cons are:

- This option is less geographically diverse. The assumption here is that the likelihood of simultaneous outages in Arizona and Kirkland from a disaster recovery standpoint (natural disaster and extreme weather) are remote.

If the City Council approves the recommended option for a secondary back at the KJC, IT's recommendation is to drop the Texas backup option immediately and set aside these funds towards the recommended KJC option. Given the high priority for IT on the ITSM and Security tracks, the implementation of the KJC strategy will take place over a 3 to 5-year time frame.

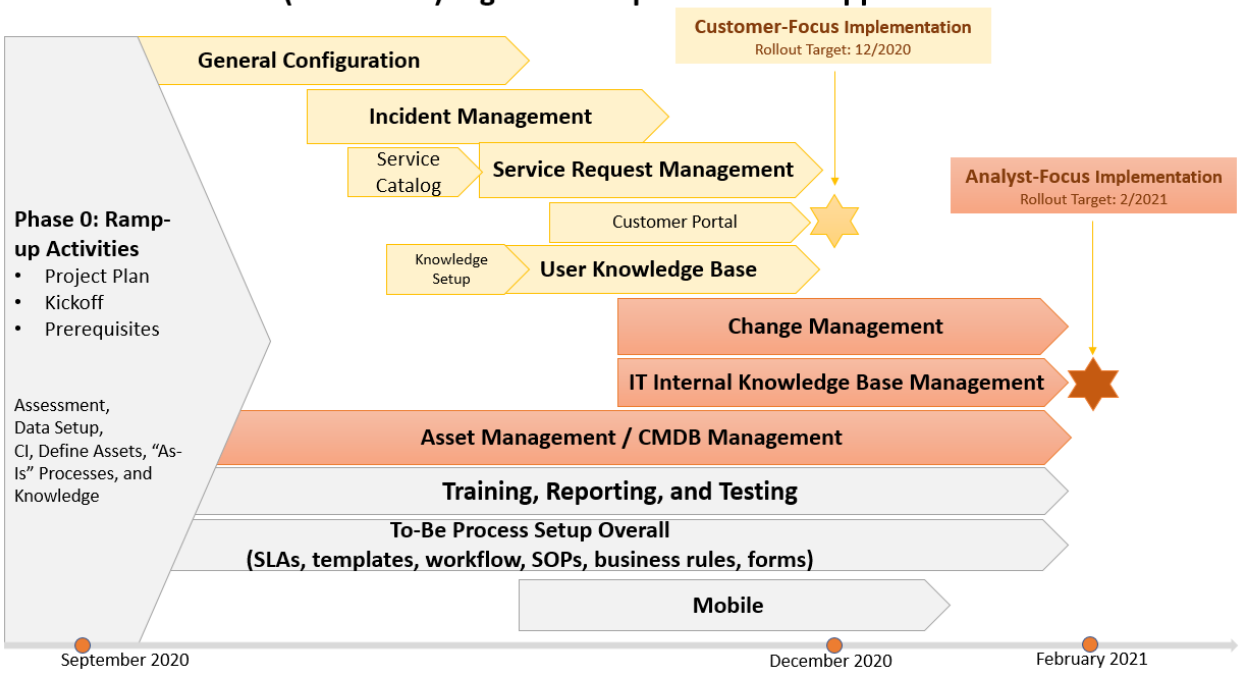
Conclusion/Next Steps:

Successes planned to be reported at the December Council Study Session include:

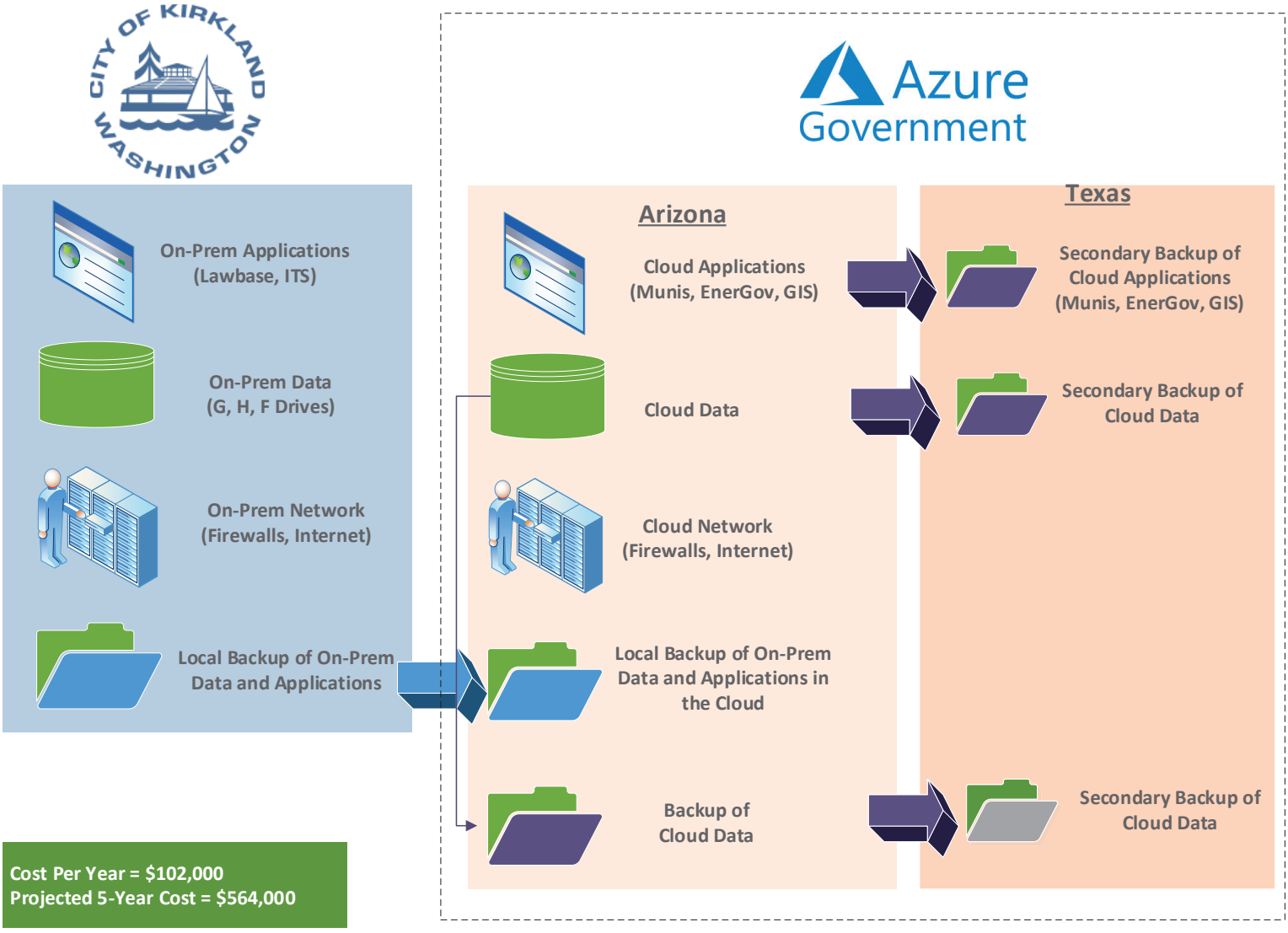
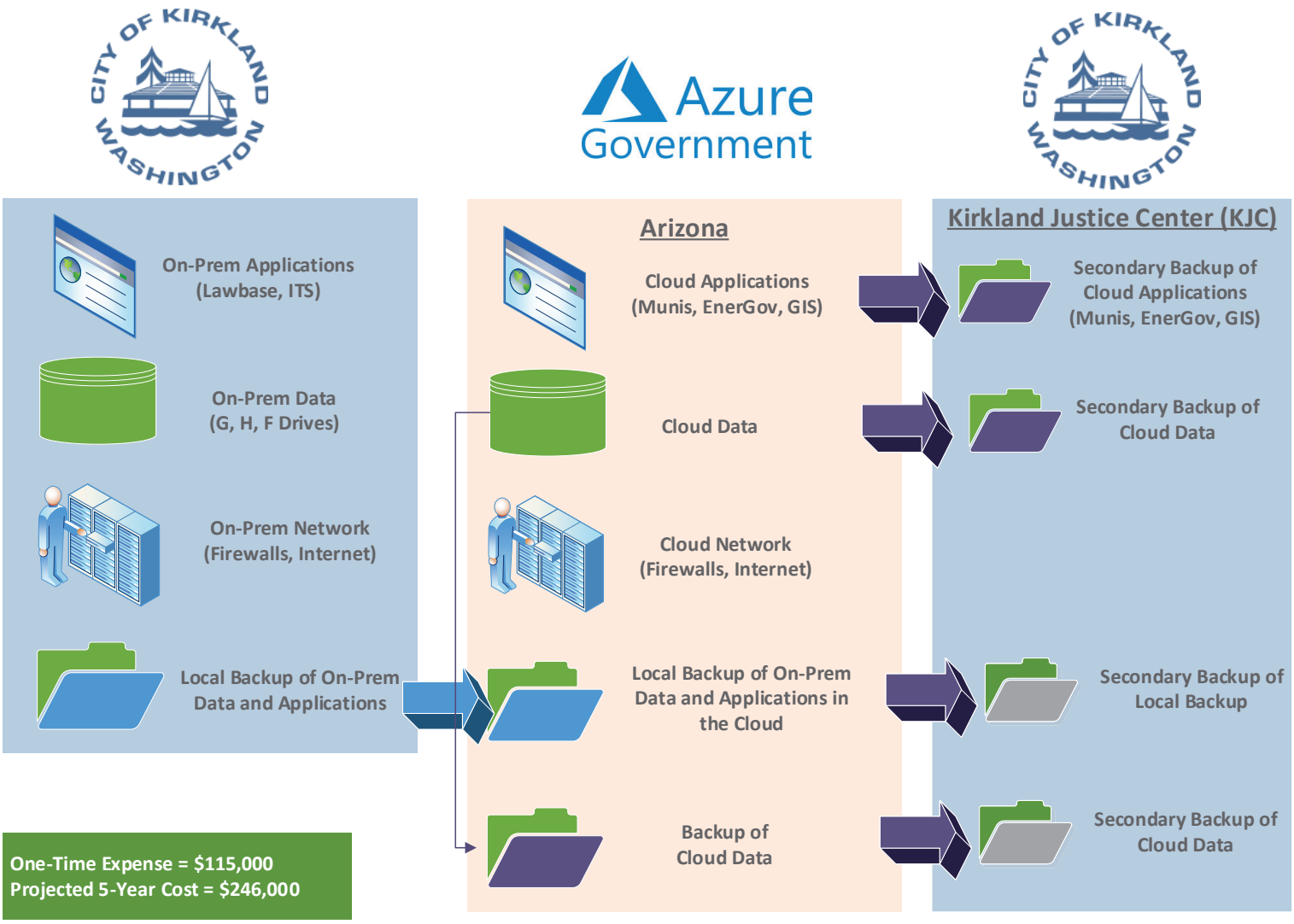
Ref.	Focal Area	Activity	By December Council Meeting
1	**IT Service Management**	Progress on implementation of new ITSM solution	✓
2	**Risk Management**	Progress on Network Infrastructure Replacement Project and other quick wins	✓
3	**Information Security Strategy and Roadmap**	Progress on work plan items recommended in the tactical roadmap	✓
		Final Information Security Strategy and Roadmap. Security related work plan items for 2021	✓
4	**Disaster Recovery and Business Continuity Planning**	Finalize alternative to Texas backup with potential funding strategy and timeline	✓

Attachments:
Attachment A – ITSM High Level Implementation Approach and Schedule
Attachment B - Current backup approach with a secondary backup in Texas
Attachment C – Recommended backup approach a secondary backup at the Kirkland Justice Center

Attachment A: ITSM (Summit AI) High Level Implementation Approach and Schedule



Attachment B: Current Backup Strategy with Texas



Attachment C: Recommended Backup Strategy