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: 01/07/2021

Subject: IT Stabilization Implementation Update #4

RECOMMENDATION

It is recommended that the City Council receive a quarterly update on the Information Technology (IT) Stabilization Project, which has been in implementation since September 2019. As a reminder, the goals of this project are:

1. Improve reliability and reduce downtime in IT operations and services
2. Continue to shift towards a mature and proactive IT culture

In December 2020, Phase 1 of Implementation was completed.

BACKGROUND DISCUSSION

At the last update to City Council in September 2020, the IT Department provided an overview of the key areas of focus for IT Stabilization:

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

This memo provides an update on activities completed in the above areas since the last update. Additionally, the memo provides an overview of major accomplishments by the IT Department in 2020.

Quick Update on Operational Stability

The increased focus on IT's Operational Stability is best reflected by a Key Performance Indicator (KPI) for IT Operations, which is the number of **Major** and **Priority 1** incidents per month. The table below records the number of Major and Priority 1 incidents for 2020.

Month	Major Incidents[1]	Priority 1 Incidents[2]	Total
Jan	3	3	6
Feb	1	3	4
March	0	3	3
April	0	2	2
May	0	2	2
June	0	2	2
July	0	0	0
August	1	0	1

Sept	2	1	3
Oct	0	0	0
Nov	1	0	1
Dec	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.			

Based on the data collected in 2020, the target for the City of Kirkland has been established as **≤ 3 for Major + Priority 1 incidents per month**. Additionally, the department has formally adopted "Incident Management" best practices and data will be recorded for the following incident types in IT's new IT Service Management Platform, SummitAI, which was launched in December 2020.

Incident Priority	Description	Target to Declare Incident	Target to Resolve Incident and Restore Service
P0 – Major Incident	Impact is Citywide or to Multiple Departments (E.g. Network down, Internet or Remote Access unavailable, etc.)	15 min	2 hours
P1 – High	Multiple Users with No Workaround available (E.g. Lucity or other Mission-Critical System is unavailable)	30 min	4 hours
P2 – Medium	Multiple Users with Workaround	90 min	8 hours
P3 - Low	Single User with No Workaround	2 hours	5 business days
P4 – Very Low	Single User with Workaround	2 hours	10 business days

Overview of IT's Major Accomplishments in 2020

Like the rest of the City, 2020 was a challenging year for the IT Department due to the COVID-19 pandemic. However, staff still delivered as planned on several key projects and initiatives, highlighted below.

No.	Project/Initiative	Date
1	Supported shift to a primarily remote City workforce	February – March 2020
2	Deployed a secure remote solution for Police Staff	February 2020
3	Optimized and reduced monthly operating costs in Azure	February – July 2020
4	Replaced on-prem storage for the City, also vacating rental space at the City of Bellevue	May 2020
5	Developed City's first formal Security Strategy and Roadmap	September 2020
6	Upgraded City's Phone System and introduced Jabber client for remote calling	September 2020
7	Deployed a new solution for Fleet and Surface Water management	September 2020
8	Received 3 NATOA Awards of Distinction for excellence in broadcast, cable, multimedia and electronic programming produced by the City	September 2020
9	Launched new Digital Evidence Storage Solution for Police	October 2020
10	Implemented OCourt to streamline virtual hearings for Municipal Court	November 2020
11	Launched new City Website	December 2020
12	Launched IT's new Service Management Platform and Customer Portal	December 2020

Update on Stabilization Implementation

1. **Risk Mitigation Activities**

As part of the IT Work Plan for 2020, several risks were mitigated and lowered to acceptable risk levels. These risks are tracked in IT's Risk Register, which was created in Q1 2020. The register is reviewed and updated by IT Management on a quarterly basis. The table below shows the distribution of risks as identified in Q1 2020 and the updated risks in January 2021. The table illustrates that several "High" and "Moderately" high risks have been successfully mitigated and shifted to a lower risk severity.

Risk Severity	As assessed in Q1 2020	As assessed in Q1 2021
High	47	31
Moderately High	31	26
Moderate	6	9
Moderately Low	1	10
Low	0	9
Total	85	85

Some key risks mitigated in 2020 are highlighted below.

Risk Category	Description	Risk Response
Vendor/Product Risk	The City's former Content Management System for the City's website was not supported by the vendor, and not on the current version, making it more prone to outages and cyber-attacks.	Risk was mitigated in two steps: 1. The former CMS was upgraded to its most current version. 2. The CMS was replaced, and the new City Website was launched in December 2020
Operations Risk	• Lack of documentation to efficiently run day-to-day operations in IT • Lack of standardized processes that follow industry standards and best practices to efficiently manage IT service delivery	Risks have been partially (50-60%) mitigated through the implementation of the City's new ITSM platform and Security Strategy and Roadmap. These risks will continue to be addressed in 2021.
Operations Risk	Knowledge gaps within and across teams on network tier, applications tier, and security.	Risks have been partially (70%) mitigated through the following activities: 1. IT Staff received ITIL Foundation 4 Training, an industry standard. 2. IT Staff were trained on the new ITSM platform with expectations to adhere to newly established SLAs for Incident and Service Management. 3. IT Staff participated in their first tabletop exercise simulating a cyberattack. These risks will continue to be addressed in 2021.
Operations Risk	In Q1 2020, the City experienced 3 outages as a result of a network storm in the local fiber loop connecting Kirkland to Bellevue, Redmond and Lake	Risks were mitigated by targeted actions taken by the Network Team. This resulted in increased network stability since Q1 2020.

	Washington School District. Additionally, we had more outages due to the network switches at City Hall being flooded. The entire City network, Express Route, Phones, City buildings, local loop connection to Bellevue, etc. are routed through these switches.	
Compliance and Security Risk	All IT system administration accounts and service accounts were stored in one application. Additionally, access permission to the application was not granted properly and several of the system accounts were not up to date.	Risk was mitigated by re-implementing access permissions based on industry best practices such as segmentation by functional workgroup. All passwords were also verified and made current.

In Q4 2020, the Risk Register was updated with 97 new security related risks as a result of the security assessment conducted by a third-party. Of these, only 4 were "High" severity and majority where "Moderate" to "Low" severity risks. One of the 4 "High" Priority risks was resolved in Q4 2020. The table below provides more information on the remaining "High" severity risks and IT's plan to mitigate these.

	Risk Description	Mitigation Task(s)	Timeline
1.	The City does not own an on-premise vulnerability scanning product or service to increase the internal scanning frequency to at least quarterly. The IT Department also does not have sufficient staff to follow up and mitigate issues raised from these scans.	IT Department purchased a vulnerability scanning tool in Q1 2020 for implementation in Q1 2021. As part of the 2021-22 Budget, an Information Security Analyst Position was added to the Network and Desktop Services Team. This position will be filled externally in Q1 2021.	Q1 2021
2.	The City does not have an IT Business Continuity Plan in place that has been agreed upon by customers.	This is a key deliverable in IT's 2021 Security Work Plan	Q2-Q3 2021
4.	The City does not have a formal security monitoring platform for the network, including log event analysis, intrusion detection alerting, and review of abberational traffic and event patterns.	As part of the 2021-22 Budget, the purchase of a Security Incident and Event Management (SIEM) platform has been funded. This is a key deliverable in IT's 2021 Security Work Plan.	Q3-Q4 2021

IT's work plan for 2021 will continue to mitigate higher-severity risks as part of the ITSM implementation, Security program and other key projects.

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

The implementation team, led by IT Deputy Director Xiaoning Jiang, went live with Phase 1 of this project on December 14th, 2020. This included the following modules:

a. Incident Management
b. Service Request Management
c. Knowledge Base
d. Customer Portal
e. Internal Dashboards and Reports

The implementation also included the development of service level agreements or SLAs tied to these modules, templates, automated workflows, Standard Operating Procedures (SOPs) and training of IT Staff. With this implementation, the IT Department now has the ability to gather data to track and report on the following Key Performance Indicators (KPIs) for IT Operations and Services in alignment with industry best practices:

No.	Key Performance Indicator (KPI)	Target[1]
1	Mean Time to Incident Resolution for P0 to P2	6 hours
2	Mean Time to Incident Resolution Target Met	80%
3	Mean Time to Service Resolution for P1 & P2	32 hours (4 Business Days)
4	Mean Time to Service Resolution Target Met	80%
5	P0 (Major) plus P1 (High Priority) Incidents	≤3 per month
6	First Call Resolution	50%
1. Targets may be modified or refined after reviewing the first year's (2021) operating data.		

The 2021 IT work plan includes the deployment of the following ITSM modules:
1. Change Management
2. Configuration Management
3. Asset Management

The 2021 work plan also includes implementing a solution for IT Operations Management (ITOM) as Phase 3 of the ITSM Implementation. 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. Funding for Phase 3 was approved by City Council as a Service Package in the 2021-22 Budget.

3. **Security Strategy**

As reported to Council previously, IT engaged CI Security to develop an Information Security Management Strategy and Roadmap for the City of Kirkland in September 2020. This effort was led by Donna Gaw, IT Manager for Security and Service Management. As part of the Security Strategy, the team met the following milestones in 2020:

1. Measured the City's cybersecurity maturity level based on industry standard
2. Developed a Security Work Plan for 2021-22 with corrective actions as identified by the vendor
3. Developed and adopted the Incident Management Plan and Policy
4. Developed six playbooks to respond to most likely cyber security incidents
5. Conducted a tabletop (TTX) exercise with all IT staff and key stakeholders from departments
6. Purchased a tool (NESSUS Professional) for vulnerability scanning
7. Developed RFP for Security Incident and Event Management (SIEM) to be purchased and implemented in 2021
8. Documented City's Network Perimeter Security
9. Completed an assessment of City's cybersecurity insurance policy. Ensured that the City is well-protected with regards to coverage for potential cybersecurity incidents.
10. Deployed Role-Based Access (RBAC) within the department – 85% complete. Completion in Q1 2021.
11. Migrating users to a more current and secure remote connectivity solution. (GlobalProtect) – 85% complete. Completion in Q1 2021.

IT's Security Work Plan for 2021 will focus on the following key tasks and projects:

a. Conduct annual penetration test by third-party – Q2 2021

b. Develop a business continuity and disaster recovery plan with a key focus on security - Q2-Q3 2021
c. Purchase and implement a solution for Security Incident and Event Management (SIEM) – Q2 to Q4, 2021
d. Implement quarterly TTXs for IT staff and key stakeholders
e. Update IT Policies to account for the "new normal" that has risen in the wake of the pandemic. Add SOPs to align with the policies.
f. Hire an Information Security Analyst to execute the security-related work plan items – Q1 2021
g. Create a cross-departmental security governance committee to keep the City's Leadership informed of security risks – Q1 2021

Conclusion/Next Steps:

The IT Department will continue to provide quarterly updates to City Council on the following areas:

Ref.	Focal Area	Activity	By April Council Meeting
1	**ITSM Phase 2 Implementation Update**	Progress on implementation of Phase 2 of ITSM solution	✓
2	**Risk Management**	Progress on Network Infrastructure Replacement Project, and other risk mitigation tasks/projects	✓
3	**Information Security Strategy and Roadmap**	Progress on 2021 security work plan items	✓