# ITS Strategic Roadmap – FY20 Planning

***Business Continuity Management (Business Continuity/Disaster Recovery)***

Author: *John Griffey*
Date last updated: *December 27, 2018*

## Background

The ITS Business Continuity Management (BCM) Program provides software solutions and guidance to the ITS department for business continuity and disaster recovery planning, including resilience strategies, assistance in determination of recovery objectives, business continuity, crisis management planning, and operational risk management considerations.

The purpose of the program is to:

- Identify risks, threats and vulnerabilities that could impact business operations
- Ensure the department has appropriate recovery strategies and plans in place to support safe evacuation of employees in the event of a disaster
- Support continuity of operations for critical IT services provided to the Metropolitan Government of Nashville & Davidson County by ITS

Business Continuity Management is an ongoing process supported by ITS senior management and resourced to ensure that necessary steps are taken to identify the impact of potential losses, manage risk, develop resiliency, maintain viable recovery strategies and plans and ensure continuity of IT services through exercising, rehearsing, testing, training, maintenance and assurance.

The BCM Program encompasses a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting ITS systems, business processes, and facility operations. The program facilitates training for ITS employees related to business continuity and disaster recovery practices, and emergency response and preparedness.

The program also administers applications used for Business Continuity/Disaster Recovery (BC/DR) processes: Assurance Continuity Manager, Assurance Notification Manager, and AboutME+.

## Current Strategic Drivers

1. **Customer Demand: High Availability** (High) – ITS customers and the residents they serve demand extremely high availability of Metro services to meet the business-critical and, for some customers, life and death responsibilities they hold.
2. **Customer Demand: Secure Government Systems** (High) – Factors including the proliferation of mobile devices, rise of hacktivism and sophisticated nation-state cybersecurity threats, and the reliance on 24/7/365 connectivity to Metro's network have increased the need to ensure the security of the Metro network, which includes addressing the availability of the Metro network and the critical services provided by Metro ITS as well as processes for assessing risk around using services.

3. **New Metro Technology: Metro Emergency and Notification System (MEANS)** (Medium) – ITS will implement in 2019 the new resident-facing emergency notification system, which will also have the capability to replace existing Sungard notification software.

## On the Horizon Strategic Drivers

1. **Construction of New Back-up Data Center** (High) – Metro is exploring buildout of a new location that could be used as a backup data center.

## Short Term Goals (0-6 months) 7/1/19– 12/31/19

| # | Goal/Objective | Est. Start | Est. Duration |
|---|---|---|---|
| 1 | **BCM Program Annual Plan Review:** Work with ITS to update business continuity strategies, emergency response and disaster recovery plans; begin development of new plans as proposed. | 7/2019 | ongoing |
| 2 | **Disaster Recovery Plan TableTop Testing:** Work with ITS department and plan development teams for tabletop testing of business continuity strategies and disaster recovery plans to identify issues and changes. | 9/2019 | ongoing |
| 3 | **Transition emergency notification solution to MEANS:** Provide support needed to migrate to the MEANS system from Assurance Notification Manager. | 7/2019 | 6 months |
| 4 | **Coordinate with External Agencies for Cybersecurity Incident Response Plan:** Collaboration efforts for new strategies, specifically the ITS Cybersecurity Incident Response Plan that requires coordination with other Metro departments. | 6/2019 | 3 months |
| 5 | **Business Impact Analysis:** Work with Metro Departments and Agencies to identify critical ITS-provided services and the assets and resources that support them. | 7/2019 | 3 months |

## Medium Term Goals (6-18 months) 1/1/20 – 12/31/20

| # | Goal/Objective | Est. Start | Est. Duration |
|---|---|---|---|
| 1 | **Disaster Recovery Plan Simulation Testing:** Work with ITS Department and plan development teams to scope, plan and then complete a simulated disaster to identify sufficiency of business continuity strategies and disaster recovery plans, while providing feedback for plan improvement. | 1/2020 | 6 months |

## Long Term Goals (18-36 months) 1/1/21 – 6/30/22

| # | Goal/Objective | Est. Start | Est. Duration |
|---|---|---|---|
| 1 | **Disaster Recovery Plan Parallel Testing:** Work with Metro Department Agencies and ITS Department plan development teams to build recovery systems and test the ability to support critical services and processes in a parallel environment. | 1/2021 | 12 months |

## Related Roadmaps

- Information Security Program
- Radio Communications

## Related Resources

- Mayoral Executive Order 34 at http://www.nashville.gov/Metro-Clerk/Legal-Resources/Executive-Orders.aspx
- Metro Government Information Security Policy at http://www.nashville.gov/Information-Technology-Services/Information-Security/Information-Security-Policies.aspx