

Town of West Brookfield

BUSINESS CONTINUITY BEST PRACTICE | JULY 2017

Report prepared By: Allison Poirier, Amelia Percentie, and Michael Hamel
Photo Credit: Wikimedia Commons – Richard B. Johnson

EXECUTIVE SUMMARY

In June of 2016, the Town of West Brookfield adopted the Business Continuity best practice as part of a Community Compact agreement signed with the Baker-Polito Administration. Working with Diane Vayda, Chairman of the West Brookfield Board of Selectmen, MassIT was able to support the Town in developing a business continuity plan (BCP), as well as a statement of work (SOW) to ensure the Town was able to effectively leverage grant funds provided through the compact. The grant enabled West Brookfield to hire a third-party vendor to complete a comprehensive IT Assessment, which included Business Continuity, Disaster Recovery and Security findings. This process provided West Brookfield with a snapshot of their current state IT environment to identify any gaps, ensure redundancy and validate their configuration.

Community Profile

The Town of West Brookfield is located in Worcester County, approximately halfway between Springfield and Worcester. Located within West Brookfield is the town beach on Lake Wickaboag, the Rockhouse Reservation with hiking and nature trails, unique craft and antique shops, and more.

Population is 3,701 residents (as of 2010 Census)

In Partnership With

Office of Municipal and
School Technology

MassIT

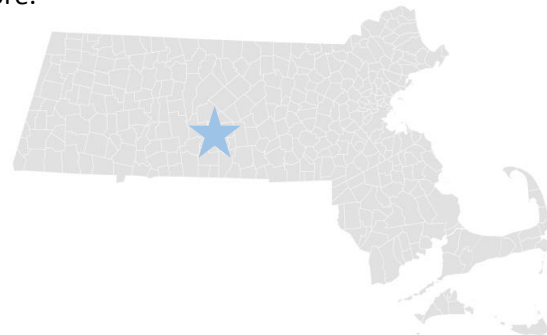




Photo Credit: Flickr – Qfamily

PROJECT OVERVIEW

On June 28, 2016, the Town of West Brookfield signed a compact with the Baker-Polito Administration that included a commitment to implement an Information Technology Business Continuity Plan (BCP). This initiative would include the development of a written disaster recovery and backup plan for critical municipal systems. The Chairman of the Selectboard, led this effort and worked with MassIT to develop a strategy and approach to developing a Business Continuity Plan. Leveraging Community Compact grant funding, the Town hired Rutter Technologies to perform an assessment of their IT infrastructure and processes. The results we presented to the Town and would inform the Business Continuity support provided by MassIT.

MassIT Engagement - Business Continuity Planning

West Brookfield partnered with MassIT to create and document a Business Continuity Plan (BCP)¹. An essential component of this engagement was the development of a Business Impact Analysis (BIA). This four-step process allows the Town to document their essential functions, and the services and systems that support them. The four steps in this process are: (1) Identify Essential Functions, (2) Develop findings for each essential function, (3) Create an Action Plan for functional gaps – findings & recommendations, and lastly (4) Develop detailed remediation plans.

¹ Business Continuity Planning or Program – The process to ensure that an organization has the ability to provide services and support for its customers and to maintain its viability before, during, and after an incident.

Step 1: Identify Essential Functions

The Chairman of the Selectboard was able to identify a list of West Brookfield’s Essential Functions. These functions were prioritized and analysis was conducted to document appropriate RTO² and RPO³ associated with each. A portion of the analysis can be seen in the table below.

Department	Essential Functions
TOWN CLERK	Issues dog licenses, marriage licenses, birth certificates, death certificates, business certificates, and conducts and maintains the Town Census. The Town Clerk's Office/ Board of Registrars registers all voters and conducts elections in strict conformance with state law. Manages online payments for Birth, Death & Marriage Certificates and Dog Licences.
TAX COLLECTOR	Timely preparation and mailing of all tax bills, and the collection and reconciliation of all municipal taxes; offers online bill payment; work closely with the Assessors, Treasurer and Accountant in performing the duties of the office under Massachusetts General Law.
POLICE	Dispatch to emergency calls, 24/7 emergency services, Firearms, Licensing, Chemical spray fee.
HOUSING	Operate according to the policies of the West Brookfield Housing Authority (WBHA), as well as the guidelines and regulations of the Commonwealth of Massachusetts, Department of Housing and Community Development. Provide public housing programs including: Elderly (667); Disabled (689) and Family (705). Screen prospective tenants for qualification, including background checks, criminal history, as well as personal and prior landlord references.
HIGHWAY	Maintain roadways, paving, improvements, ice and snow removal.
BOARD OF HEALTH	Work with State DPH, and other agencies to ensure public safety, provide screenings, publish information regarding public health and safety issues, work with other agencies to ensure public awareness and safety.
TREASURER	Plans and directs the receipt, accounting and disbursement of all town funds; invests all town funds, and other special funds, with an emphasis on

² RTO – Recovery Time Objective, is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

³ RPO – Recovery Point Objective, describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan’s maximum allowable threshold or “tolerance”.

	<p>yield, safety, and liquidity.</p> <p>Monitors cash levels in the treasury; responsible for borrowing funds for the town and arranges temporary or longterm borrowing of funds, as necessary, for town needs; pays interest and maturing debt; signs bonds, notes and other papers of credit for the town both short-term and long-term; ensures that all necessary paper work is in place.</p> <p>Receives deposits from various sources having to do with town business; reconciles statements and makes deposits; transfers funds; pays bills, employee payrolls, and local obligations; invests town funds.</p> <p>Prepares requests for proposals for banking services to be provided to the Town.</p> <p>Responsible for tax titles, receipt of payments, discharge of tax titles and foreclosures. Maintains tax title records.</p> <p>Maintains custody of securities for trust funds; collects, accounts for, and invests income from investments in fund portfolios.</p>
FIRE	Dispatch to fire related emergencies, 24/7 emergency fire and related services.
LIBRARY	<p>24-hour surveillance with closed circuit televisions around the interior of the building, Allow patrons to access their library accounts online and renew items, order materials, and view the online catalogs of all member libraries in central and western Massachusetts, ensure that West Brookfield library cards are accepted at all member libraries.</p> <p>Offer the following resources to constituents:</p> <p>Library Card, Catalogs, Interlibrary Loan⁴, Commonwealth Catalog⁵, Digital Catalog⁶, Magazines, Book Sale, Kindle/Sony E-Reader/Nook, Computers & Other Equipment, Free Public WiFi, Printers, Scanner, Copy Machine, Fax Machine</p>

⁴ Interlibrary Loan – Reserve books from other MA libraries; pick up and drop off at any participating library.

⁵ Commonwealth Catalog – Catalog includes libraries in other MA locations.

⁶ Digital Catalog – Borrow eBooks and eAudio Books for 2 weeks.

Step 2: Develop Findings

West Brookfield's applications are hosted by external 3rd parties and because these applications live in other vendor's cloud environments, the key obstacle for West Brookfield is to define the means in which users would connect to these applications, in a disaster event. This would need to be incorporated in West Brookfield's BCP plan documents.

Step 3: Create Action Plan for Functional Gaps (Findings/Recommendations)

West Brookfield attended the MassIT Workshop series, and began their BCP documents. Within the Disaster Recovery Plan, the identified gap (outlined in Step: 2-Develop Findings) will be incorporated.

Step 4: Detailed Remediation Plan

West Brookfield will complete their required BCP plans consisting of: Business Impact Analysis, Emergency Response Plan, and Disaster Recovery Plan, within 6 months. It was recommended that once West Brookfield completes their Emergency Plans, they should identify a location that can be used as a Disaster Recovery rally point. Going forward, West Brookfield should routinely test connectivity levels to their applications.

IT Assessment

West Brookfield hired Rutter Technologies to complete their IT Assessment. The purpose of the engagement was to examine the Business Continuity, Disaster Recovery and Security practices currently employed at the Town and to provide recommendations.

Business Continuity and Disaster Recovery (BCDR)

The assessment report touches on several disaster contingencies, including but not limited to: power outages, IT system crashes, file corruption, and hardware failures. Because BCDR consists of several stages and is typically funding driven, the focus of an organization should not necessarily be perfection in any one area, but a constant revision of where funding can be most impactful to reach the organization's specific BCDR goals.

Most organizations prioritize backup systems since they provide the best value in terms of coverage and capability. Once the systems are stabilized, advanced protection technologies are implemented to lower RTO and RPO for essential applications and systems, then incrementally for the rest of the systems. By looking at West Brookfield's business processes, Rutter was able to identify critical applications using objective measures such as: Financial loss, legal and regulatory issues, and customer impact.

Key Findings and Recommendations:

Rutter discovered that essentially all of West Brookfield's applications are hosted by external 3rd parties. Because these applications live in another other vendor's cloud, the key obstacle for West Brookfield would be to define a BCDR strategy and the means in which users would connect to these applications. With vendor hosted external applications, concerns regarding disaster impact are alleviated; however, there is work that West Brookfield can continue to address that will benefit the Town in the event of a disaster.

It was recommended that once West Brookfield completed their Emergency Plans, they should identify a location to be used as a Disaster Recovery rally point. The Town examined their existing vendor support contracts to determine the limitations of afterhours support, SLAs, etc. Having this information on hand ensured that the Essential Functions listed in the BIA document could be supported by their associated vendors.

Network and Security

The network is the backbone of any IT infrastructure and should be stable to support the growth of an organization. Throughout the assessment, redundancy was evaluated alongside the following criteria:

Layer 1 – Physical

- Are the devices in use considered enterprise class
- Are the devices in use under manufactures support contract in case of hardware failure
- For each device interconnect, do they have dual connections between each other

Layer 2 – Data Link

- Are the devices considered ‘managed’ network devices
- Is each device capable of using VLANs for network segmentation

Layer 3 – Network

- How routing is controlled within the environment
- Are there multiple paths and redundancy designed within the environment for access to business critical applications and the internet

The critical components to a secure IT environment are access controls, visibility, and response. Rutter’s Security review was performed to provide high-level insight into the Town’s security posture, evaluating fifteen areas that determine the health of the three main IT components:

1. Evaluation Criteria

- Inventory of Authorized and Unauthorized devices
- Does the organization have an actionable inventory of devices on their network
- Does the organization have logging enabled for their DHCP services to provide knowledge of what devices were active on the network at any given time
- Does the organization have a Bring Your Own Device policy and how is it enforced

2. Inventory of Authorized and Unauthorized Software

- How is software updating performed
- Does the organization have support contracts for their software (allowing for upgrades and patches)
- Is there an actionable list of authorized software installed on each system
- Can the end user install software on their own workstation without approval

3. Secure Configurations of Workstations and Servers
 - Are workstations and servers deployed from images
 - Are images updated regularly with software updates and patches
 - How is patch deployment performed
 - What are the procedures for remote administration of workstations and servers
4. Vulnerability Scanning
 - Are there vulnerability scanning tools in place
 - What is the remediation time for vulnerabilities found in systems
5. Malware Defenses
 - What antimalware tools are in use
 - Is central management and reporting in place for the antimalware tools
 - Are attachments for emails scanned prior to allowing them into the organization
6. Wireless
 - What method of authorization and encryption is used for internal wireless networks
 - What is the method used to provide guest wireless access
7. Skills Training
 - How often is security awareness training performed for the users
 - How often is technical security training provided for the IT staff
8. Secure Configuration of Network Devices (switches/routers/firewalls)
 - What is the organization's firewall policy for permitting and denying traffic to and from the internet
 - What method is used to authenticate to all network devices
9. Limitation and Control of Network Ports and Services on Each System
 - Is a software firewall deployed on workstations and servers
 - Is there a process in place for port scanning to determine if any new applications are deployed
 - Are there hosted services within the organization that are visible from the internet and how they are secured
10. Administrative Privileges
 - Are there separate accounts in place for administrators day-to-day activities from their administrative tasks
 - How is password complexity enforced
 - Do the users have administrative rights to their own workstations

11. Boundary Devices

- Does the organization use a next generation firewall (NGFW)
- How often are the advanced features updated (such as IPS, Antimalware)
- Does the organization have remote access via VPN or other method configured

12. Maintenance and Monitoring of Device Logs

- Does the organization use a central logging server for all devices
- What is the current log retention policy for all devices
- Do the devices all have their times synchronized for the purpose of log timestamping

13. Controlling Access Based Off Need to Know

- Do the organizations critical functions have limited access to only those that require access
- Is there audit logging in place for these functions to know who accessed them, from where and for how long

14. Account Monitoring and Control

- Is there a process in place for account creation/modification/deletion
- Are screen locks enabled on all systems
- How often is a review conducted of all active accounts within the organization
- What is the current lockout policy for incorrect logins

15. Incident Response Planning

- Is there a documented incident response plan in place
- When was that plan last tested for accuracy

Following the Network and Security assessment, West Brookfield received a moderate score to reflect the maturity of their network environment. They scored slightly below average in the Security assessment.

CONCLUSION

The Town of West Brookfield has taken significant steps toward improving business continuity for their internal and external users. By completing the BCDR and Security assessment with Rutter Technologies and building out their Emergency plans, the Town is better positioned to address any gaps that currently exist in their IT environment. With many initiatives underway, the Town continues to adopt best practices and ensure essential services are available to constituents. West Brookfield's ability to recover essential systems and services in the event of a disaster has been validated by the Assessment completed by Rutter.