The Public Sector client for this case study is located in Southwest Ontario. Over the course of a few weeks, GDL studied the client’s Ad Hoc recovery plans information and ran it through our customized Systematic Framework. Not surprisingly, changes were required and it was less about new technology than it was about understanding the business requirements and leveraging investments in people, process and technology to develop an IT culture of resiliency and adaptability for Emergency Management and DR preparedness. Other discoveries included non-compliance with regulatory standards and Business Impact Analysis to establish recovery time objectives. GDL mitigation measures were recommended that involved a reasonable budget and a phased approach starting with mission critical services.

Executive Summary

This Case Study is based on an actual engagement for which GDL Solutions was contracted by a public sector organization in Southwest Ontario to develop a Disaster Recovery Readiness Assessment.

The client wanted to be better prepared for a disaster, based on faster paced, on going threats from various sources that are less predictable than previous eras. The purpose of the Readiness Assessment was to assist in diagnosing what mitigation measures should be considered to overcome existing technical and non-technical deficiencies in order to establish an effective Disaster Recovery and Business Continuity Plan for the organization.

While working with the Client, GDL designed a framework that enabled the client to maximise ROI on current and future investments to improve their Emergency Management preparedness through better focus on their people, process and technology. The assessment was used as a building block to creating a more comprehensive Business Continuity Plan.

Due to the confidential nature of this case study, the client’s name and other details are not disclosed or published.
Methodology
GDL’s “DR Readiness Assessment” closely follows a 5-Step process. The details of each step were developed in a consultative and cooperative manner by a team from GDL and the Client. The steps were: **Planning, Visioning, DR Readiness, Sharing Findings** and **Future Steps**.

The starting point for this assessment was to develop a scope of work based on where they are currently. In most cases, the Client needs to simultaneously plan for disaster recovery as it also concentrates on keeping the lights on. Thus, GDL used a holistic approach involving the client’s **People**, **Process** and **Technology** to develop a framework for analysis.

The **People** component involves resourcing and skills development to identify the right expertise required to properly implement, maintain and periodically test the Client’s DR plans. Executing their DR strategy would increase IT staff workloads, and Clients need to plan for flexibility and perhaps additional benefits for participating staff. The **Process** component is likely the most difficult to address as generally it revolves around best practice, GDL’s industry knowledge and experience to develop a checklist of activities and steps to undertake to successfully recover from an incident. The **Technology** component involves both infrastructure and application architectural considerations that would equip their success.

Vision for DR – with upper management support
The tone from the top and involvement for critical decisions, overall project direction and milestone achievements are essential to the overall success of the DR program. Management should have a clear vision of IT’s role in the organization’s ability to recover from a disaster that includes the development of a cohesive structure (people, process and technology) for an effective recovery plan. GDL was pleased to provide input to the vision.

Typical Engagement Process
GDL modeled its Readiness Assessment for the Client from industry best practice approaches, which were then manifested in a **DR Readiness Assessment Framework** that expands on the five essential steps to a meaningful and credible design.

The Readiness Assessment was intended to be action oriented and for this reason the DR Readiness Assessment Framework was instrumental in identifying and confirming the client’s existing deficiencies and to outline a range of options available to the Client to mitigate them.

The framework for the assessment was subject to detailed consultative discussions with the Client’s IT staff. For each significant deficiency, GDL proposed a concept or a set of mitigating measures that formed the basis of a DR Action.
Plan by the Client. The mitigating measures proposed were empirically based, specifically on best practices. It also incorporated the needs and experiences of both the Client and GDL to date.

**How prepared is IT for DR?**

In a Readiness Assessment exercise, it is always prudent to get back to the fundamental elements for analysis that revolves around People, Process and Technology. The Readiness Assessment can be designed to accommodate or deal with many detailed aspects of each of these three elements depending on the complexity of the organization, available resources for the analysis and scope of the undertaking. It should be noted that a Comprehensive Readiness Assessment is much more broad and extensive in scope than this specific Case Study. GDL uses templates and questionnaires that cover as many aspects of the Client’s DR planning as possible. The Readiness Assessment by GDL for the Client in this Case Study is limited in scope and duration by virtue of time that the Client’s IT Staff could expend as well as by the resources that were available.

The main purpose of this Readiness Assessment is to identify the existing deficiencies in the Client’s organizational readiness to deal with a full disaster or technology incident and subsequently, to examine the range of available options to mitigate against these deficiencies and to select technical and non-technical solutions to increase the readiness of the Client. Of necessity, the solutions may span a continuum ranging from simple implementable actions to those that may be very difficult if not impossible to deploy. Furthermore, analysts performing the solution should be familiar with and implement from the lens of ever-changing technology.

GDL started the engagement by first developing a simple framework for analysis based on the understanding set out above. The questions posed in the **DR Readiness Framework** under each of the three elements of People, Process and Technology were customized based on discussions with the Client.

A schematic of the DR Readiness Assessment Framework is presented in **Appendix A**. There were numerous pages of elements of the Readiness Assessment that went into this Framework. These of course, cannot be shared in this Case Study due to Privacy considerations.

In this GDL Case Study, each element of the Framework was subjected to rigorous review and discussion. Then, GDL summarized their comments, observations and suggestions for mitigating the deficiencies in three distinct sections – **Current State, Deficiencies** and **Mitigation Measures**.
Current State and Deficiencies
The following are illustrative examples of discussion topics that were documented by GDL regarding the current state and deficiencies based on field work and extensive discussion with the Client:

- Emergency Preparedness of the Organization as a whole
- Business Continuity Plan or Program (BCP)
- DR Plan development
- Staff Training and matching skillsets to DR needs
- Business Impact Analysis BIA to assign level of criticality RTO’s RPO’s as validated by business leaders
- DR Coordination function
- RPO and RTO and the scale of Incidents
- Data Center Protection
- Move to Cloud and the Hybrid Strategy
- DR Plan: Assess, Recover, Resume and Review
- Technology teams make the call
- IT Department must identify the resources requirement

Mitigation Measures
GDL Solutions took each of the 3 elements of the Framework – People, Process and Technology – and described in detail our best practice approach to define mitigating measures. Below are illustrative examples of each of these:

- The Emergency Preparedness and the need to involve IT
- Senior Management Commitment is key
- Define and build the DR recover management team
- Define roles of the Support Departments such as HR & Communications
- DR Plan testing
- Define the IT Crisis Management Centre
- Document the DR process: Assess, Recover, Resume and Review
- Establish IT recovery timelines
- Verify technical aspects of Readiness Assessment

DR Plan Testing
Disaster recovery planned testing and reviews are an essential part of the DR development process. Building a quality IT disaster recovery plan is a team activity, so recurring practice and testing maintain continuous awareness and competence and are critical to a successful recovery as non-technical changes can affect the plans. We suggested to the client that such reviews:

1. Reflect any updated organizational priorities, changes or goals
2. Ensure that all team lists are up to date
3. Ensure that call lists are up to date
4. Confirm that configuration changes in the environment have been made.

The goal of a good disaster recovery plan is that it can be executed smoothly and effectively at any time. To make this happen, we indicated to the Client that everyone that has a role to play in the plan should be involved in testing to gain experience through practice.

The disaster recovery plan should be tested annually to include a table top walkthrough, disaster simulation, or full failover testing.
Observations and Recommendations

GDL concluded that, while the Client’s IT department staff has been active and effective in understanding their DR challenges, the organization has – like most other Public Sector organizations in Ontario – some way to go to be Risk Aware and Disaster Ready.

The areas for improvement regarding DR Readiness were effectively illustrated on the Readiness Assessment Framework.

The Client was requested to use this Readiness Assessment conducted by GDL as a major step towards a Comprehensive Disaster Recovery Plan.

The following action items were recommended based on the key needs of the Client:

1. Resolving the implications of a Single Hub for the Client’s Network
2. Options for Cloud vs. Secondary DR Site vs. Do Nothing
3. Replacement considerations of existing back-up systems
4. Options for data archiving
5. Client had a lot of available resources and well planned steps would significantly improve their DR readiness at no extra cost
6. Larger items need budget, effort and time to complete.

In summary

The Client confirmed to GDL that our Assessment put into context where they need to be and they now have a more detailed approach to interconnect their business unit requirements with IT procedures in a comprehensive process from incident to recovery with periodic testing to make sure it works.

About the Authors:

Zoreena Abas is an entrepreneur with over 20 years of IT leadership experience and a strong focus on customer satisfaction. She received her MBA from the Richard Ivey School of Business, and an ICD.D designation in director leadership and corporate governance from Rotman School of Management.

Dr. Louis Shallal Dr. Shallal serves as an Executive Advisor with GDL Solutions. Prior to his current role, he was the CIO for the Government of Jamaica overseeing the IT function for the entire government and almost 1,000 IT professionals serving some 115,000 employees. Also, Dr. Shallal served for eight years as the CIO for the Regional Municipality of York, and CIO for the City of Hamilton and enjoyed a career with the Region of Ottawa-Carleton as an Executive Director of IT. Dr. Shallal has a Ph.D. in Civil Engineering from Carleton University Canada; an MSc from Wayne State University, and holds a diploma from a Program for Senior Executives in State and Local Government from the Kennedy School of Government at Harvard University.
# Appendix A

<table>
<thead>
<tr>
<th>Color code legend:</th>
<th>Green (G)</th>
<th>Yellow (Y)</th>
<th>Red (R)</th>
<th>Grey (O)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Easily doable with minimal resources</td>
<td>Doable with additional effort &amp; resources</td>
<td>Difficult to implement &amp; requires significant resources</td>
<td>Insufficient information /needs further investigation</td>
</tr>
</tbody>
</table>

### Elements of The Readiness Assessment

<table>
<thead>
<tr>
<th>Identified Deficiencies For DR</th>
<th>Range of Mitigation Options and Technical Solutions</th>
<th>Selected Mitigation and Technical Solution</th>
<th>Color code</th>
<th>Comment and/or Questions NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>For Discussion with Client. Comments are presented first followed by questions.</td>
</tr>
</tbody>
</table>

### PEOPLE / PROCESS / TECHNOLOGY

- Is there a BCP document?
- How is the BCP process initiated with the Fire chief?
- Are Tabletop/mock exercises conducted (and documented) on an annual or periodic basis?
- Is there any involvement by the BCP with the IT DR planning process?
- Who would have access to the essential passwords?
- Who is authorized to make the Disaster/emergency declaration?
- Where are the DR execution plans kept?


- Is the DR process documented regarding the 3 elements?
- Is there an already developed and documented IT DR plan?
- Has business impact analysis, assigned level of criticality, and RTOs/RPOs been validated by business leaders?
- Has a threat-risk assessment (TRA) for the IT environment been carried out?