



# Proposal: Microsoft Power Platform & Dynamics 365 Sales Professional Implementation Project

For Leonardo Company Ottawa - Federal Government Entity

Prepared by Cloudstrucc Inc.

## Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>2</b>
<b>SCOPE OF WORK .....</b>	<b>2</b>
<i>Core Dynamics 365 Sales Professional Implementation.....</i>	<i>2</i>
<i>Power Platform Security Hardening .....</i>	<i>3</i>
<i>JIRA Integration &amp; Workflow Automation .....</i>	<i>3</i>
<i>Advanced Security &amp; Compliance .....</i>	<i>3</i>
<i>Training &amp; Documentation.....</i>	<i>4</i>
<b>PRE-REQUISITES AND DEPLOYMENT APPROACH.....</b>	<b>4</b>
🔑 <i>Access and Privileged Roles .....</i>	<i>4</i>
🔧 <i>Cloudstrucc Build &amp; Staging Environment Model .....</i>	<i>4</i>
🔒 <i>Protected B Security Requirements .....</i>	<i>5</i>
<b>DURATION AND PHASING.....</b>	<b>6</b>
<i>Project Duration: 45 to 90 Calendar Days .....</i>	<i>6</i>
<b>IMPLEMENTATION COST ESTIMATE (CAD).....</b>	<b>6</b>
<b>LICENSING REQUIREMENTS (CAD PRICING) .....</b>	<b>8</b>
<i>Microsoft 365 &amp; Dynamics 365 Licensing (CAD).....</i>	<i>8</i>
<i>Power Platform Security Add-ons .....</i>	<i>9</i>



# Executive Summary

Leonardo Company Ottawa requires a comprehensive Customer Relationship Management (CRM) solution that aligns with Canadian federal government security standards and operational requirements.

To deliver secure, compliant, and mission-critical CRM capabilities, the implementation must ensure alignment with:

- **Government of Canada Directive on Security Management** (Protected B requirements)
- **Treasury Board Cyber Security Event Management Plan**
- **ITSG-33** IT Security Risk Management framework
- **ISO/IEC 27001** and **NIST 800-171** international standards
- **Controlled Unclassified Information (CUI)** handling guidelines
- **PIPEDA** privacy protection requirements
- **Cloud Security Assessment and Authorization (CSAA)** framework

This proposal outlines how Cloudstrucc will implement a **Microsoft Dynamics 365 Sales Professional and Power Platform solution** that creates a **fully secure, Protected B-compliant CRM environment** with advanced threat protection, data loss prevention, customer-managed encryption keys, and **network isolation using Azure Private Endpoints and Virtual Network (VNET) integration**.



These enhancements ensure data sovereignty, prevent unauthorized access, and provide granular control over Microsoft 365 and Power Platform traffic through approved network pathways — critical requirements for aligning & complying with the security standards listed above.

The end state will position Leonardo Company Ottawa with a secure, modern, and scalable CRM platform that maximizes existing Microsoft 365 E5 investments while ensuring comprehensive compliance with federal security regulations and seamless integration with existing JIRA on-premises infrastructure, including project/task mapping and budget module connectivity for enhanced financial visibility from lead generation through project completion.

**Important Note:** This proposal is based on high-level requirements gathered to date. Final scope and implementation details will be refined during the discovery phase to ensure all specific organizational needs are addressed.

## Scope of Work

### Core Dynamics 365 Sales Professional Implementation

-  Deploy and configure Dynamics 365 Sales Professional with Protected B compliance
-  Implement comprehensive contact management and opportunity tracking



- ☒ Configure sales pipeline automation and opportunity management
- ☒ Setup advanced analytics and reporting with Power BI integration
- ☒ Enable custom entity creation and workflow automation

### **Power Platform Security Hardening**

- ☒ Configure Power Platform environments with Protected B security controls
- ☒ Implement Azure Private Endpoints for Power Platform services
- ☒ Enable VNET integration for secure network isolation
- ☒ Apply Microsoft Purview policies (DLP, auto-labeling, encryption)
- ☒ Configure Customer Managed Keys (CMK) for data encryption
- ☒ Setup Conditional Access and session controls
- ☒ Enforce managed device compliance for platform access





### **JIRA Integration & Workflow Automation**

- ☒ Design and implement bi-directional JIRA on-premise integration via On-Premises Data Gateway
- ☒ Configure Power Automate flows for real-time data synchronization
- ☒ Setup budget module connectivity and financial workflow automation
- ☒ Implement project and task mapping between JIRA and Dynamics Sales pipeline
- ☒ Enable automated case escalation and status updates
- ☒ Implement custom field mapping and data transformation

### **Advanced Security & Compliance**

- ☒ Configure Sensitivity Labels (client-provided or default Protected B classifications)
- ☒ Implement Data Loss Prevention (DLP) policies
- ☒ Enable Microsoft Defender for Office 365 and Power Platform
- ☒ Configure comprehensive audit logging and retention policies
- ☒ Implement Protected B data classification and handling
- ☒ Setup security monitoring with recommendations for SIEM integration (client responsibility)

## Training & Documentation

-  Deliver comprehensive user training and administrator guides
-  Provide security best practices documentation
-  Conduct knowledge transfer sessions
-  90-day support period with optional extension

# Pre-Requisites and Deployment Approach

To perform the activities outlined in this proposal, the following pre-requisites and operating model must be established:

## Access and Privileged Roles

Cloudstrucc will require:

- A dedicated **privileged administrative account** or membership in a **privileged role group** within Microsoft Entra ID.
- The following roles or equivalent custom RBAC assignments:
  - **Global Reader** (for assessments and baselining)
  - **Security Administrator** (for configuring Defender, alerts, Purview)
  - **Compliance Administrator** (for DLP, Sensitivity Labels, eDiscovery)
  - **Dynamics 365 Administrator**
  - **Power Platform Administrator**
  - **SharePoint Administrator** (for integrated document management)
  - **Privileged Role Administrator** (for conditional access configuration)
  - **Azure Network Contributor** (for private endpoint and VNET provisioning)
  - **Application Administrator** (for JIRA integration setup)
- Access to an on-premises user account for JIRA integration build

Access must be granted by the Leonardo Company Ottawa Entra/AD administrator(s) prior to the build activities & deployment to the organization's Azure/M365 tenant.

## Cloudstrucc Build & Staging Environment Model

To support structured, low-risk implementation aligned with federal change management requirements:



- Cloudstrucc will use its **own Azure subscription and Microsoft 365 tenant** for initial **build, configuration, and templating**.
- This isolated tenant will mirror Leonardo Company Ottawa's Protected B compliance requirements and baseline.
- Implementation phases:
  - **Development Environment:** Initial configuration and testing in Cloudstrucc tenant
  - **Client Staging Environment:** Validation in client test tenant or sandbox
  - **Production Deployment:** Controlled rollout using Infrastructure as Code (IaC) templates

**Configuration artifacts will include:**

- **ARM/Bicep templates** for Azure resource provisioning
- **PowerShell scripts** for Power Platform configuration
- **Custom D365 build artifacts, Power Automate & Plugin solutions (unmanaged & source in organization's code repository)** for JIRA integration
- **Compliance policy templates** for Protected B requirements

**This model ensures:**

- Minimal disruption to existing Leonardo Company Ottawa services
- Compliance with federal change management protocols
- Reproducible security posture across environments
- Audit trail for all configuration changes

## **Protected B Security Requirements**

The implementation will address specific Protected B requirements:

- **Data Sovereignty:** All data remains within Canadian geographic boundaries
- **Encryption Standards:** AES-256 encryption at rest and TLS 1.3 in transit
- **Access Controls:** Multi-factor authentication and conditional access policies
- **Network Isolation:** Private endpoints and VNET integration
- **Audit Compliance:** Comprehensive logging and retention policies
- **Incident Response:** Integration with government security operations centers



# Duration and Phasing

## Project Duration: 45 to 90 Calendar Days

Phase	Duration	Milestone	Outcome
Phase 1	Week 1-2	Discovery & Protected B Assessment	Gap analysis and compliance baseline
Phase 2	Week 3-4	Core D365 Sales Professional Deployment & Build	CRM foundation with basic security controls
Phase 3	Week 5-7	Power Platform Security Hardening	Protected B compliance and network isolation
Phase 4	Week 5-11	JIRA Integration & Workflow Automation	Bi-directional sync and automated workflows
Phase 5	Week 11-13	Advanced Security & Compliance	Full DLP, labeling, and monitoring active
Phase 6	Week 13-14	Testing, Training & Documentation	User training, documentation, handover
Final	Day 90	Go-Live & Support Transition	Production ready, support period begins

# Implementation Cost Estimate (CAD)

Implementation timeline and costs to be finalized based on detailed requirements gathering.

Item	Description	Estimated Cost (CAD)	Estimated Due Date
			(duration post award)



Discovery & Protected B Compliance Assessment	Security audit, gap analysis, compliance mapping	\$5,000.00	Mid-Late September
Dynamics 365 Sales Professional Setup	Core CRM deployment, configuration, customization	\$10,000.00	Mid-Late September
Power Platform & Azure Artifacts Security Hardening  & Configuration	Private endpoints, VNET integration, CMK setup	\$7,000.00	Mid-Late October
JIRA Integration Development & advanced build workflows  for Dynamics 365 to meet integration requirements	Bi-directional sync, budget module connectivity	\$12,000.00	Mid-Late October
Advanced Security Configuration	DLP, labels, monitoring, incident response setup	\$4,500.00	Early November
Data Migration & Legacy System Integration	Data import & cleansing	\$5,000.00	Mid November
User Training & Change Management	End-user training, admin training, adoption support	\$3,000.00	Mid-Late November
Documentation & Knowledge Transfer (for admins)	Admin guides, user manuals, security procedures	\$3,500.00	Early December
Support (90 days)	Post-implementation support, tuning, optimizations	\$5,000.00	December-March (2026)
<b>Subtotal</b>		<b>\$55,000.00 CAD</b>	



HST (13%)		<b>\$7,150.00 CAD</b>	
<b>Total with HST</b>		<b>\$62,150.00 CAD</b>	

**Payment Terms** The total amount indicated in this proposal, including applicable taxes, shall become payable upon completion of the scope of work as outlined herein. Payment schedule will align with federal government procurement policies and milestone-based deliverables. Final payment shall be due within thirty (30) days of the client's written confirmation of acceptance and sign-off of the completed deliverables. This agreement shall be governed by the laws of the Province of Ontario and the federal laws of Canada applicable therein.

Optional extended support available at negotiated hourly rates

## Licensing Requirements (CAD Pricing)

### Microsoft 365 & Dynamics 365 Licensing (CAD)

**Pre-requisite:** All users must have Microsoft 365 E5 licensing as the foundation for this implementation.

License Component	Features Required	Estimated Monthly Cost (CAD/user)
Dynamics 365 Sales Professional	Core CRM functionality, sales automation	~\$65
Power Apps Premium / Power Automate Flow  for extended compute (TBD - depending on  complexity / throughput of integration)	Advanced connectors, extended compute	~\$30
Microsoft Defender for Business Apps	Advanced threat protection for Dynamics 365	~\$4





## Power Platform Security Add-ons

Security Component	Purpose	Estimated Monthly Cost
Customer Managed Keys (CMK)	Enhanced encryption control for Protected B	~\$500/month
Private Endpoint Connectivity	Network isolation and VNET integration	~\$200/month
Power Platform DLP Premium	Advanced data loss prevention policies	Included in E5
Microsoft Purview Information Protection	Sensitivity labeling and classification	Included in E5