Government of Canada | Gouvernement du Canada

DIGITAL TRANSFORMATION & IM/IT EFFICIENCY STRATEGY

Ministerial Briefing & Talking Points

📅 **Document Date:** June 24, 2025
🔐 **Classification:** Protected A
👤 **Prepared for:** Federal Minister Meeting
📊 **Subject:** Strategic IT Cost Reduction & Digital Transformation

💰 **POTENTIAL SAVINGS:** 5-10%+ Annually on IM/IT spending (across every budget type)
⚡ **SERVICE IMPROVEMENT:** 60-80% Faster Delivery
🛡️ **SECURITY ENHANCEMENT:** Centralized & Standardized
📈 **LICENSE UTILIZATION:** From ~30 to 80%+

EXECUTIVE BRIEFING DOCUMENT

Digital Transformation & IT Efficiency Strategy

Protected A

Executive Summary

The federal government can achieve billions in cost savings and dramatically improve service delivery by leveraging existing Microsoft E3/E5 licenses, adopting SaaS-first strategies, eliminating redundant

security assessments, and implementing accountability-driven procurement practices. **Bottom Line**: We're paying for premium tools but using them at basic levels while simultaneously overpaying for custom solutions that could be built efficiently using existing platform capabilities.

1. Massive Underutilization of Existing Microsoft E3/E5 Investments

The Opportunity

Most federal employees have E3 or E5 licenses but agencies are only using ~30% of available capabilities, while simultaneously paying consulting firms millions to build custom applications.

Key Capabilities Not Being Leveraged

Microsoft 365 E3 ($36/user/month) includes:

- Power Apps: Build custom applications without coding
- Power Automate: Automate workflows and processes
- Power BI: Data analytics and reporting
- SharePoint: Document management and collaboration
- Microsoft Teams: Advanced collaboration features
- Dataverse for Teams: Database capabilities

Microsoft 365 E5 ($57/user/month) adds:

- Advanced security tools (Microsoft Defender suite)
- Advanced compliance and data governance (Microsoft Purview)
- AI-powered analytics
- Advanced identity management (Azure AD Premium P2)
- Power BI Pro: Enterprise analytics capabilities

The Waste

- **ArriveCAN lesson**: A simple app that could have been built using Power Apps + Power Automate in weeks, not months, and for thousands, not millions
- Government paying consulting firms $1,000+/day to build basic CRUD applications that citizen developers could create using existing E3/E5 tools

- ArriveCAN cost ballooned from $80,000 to nearly$60 million for functionality achievable with existing licenses

2. SaaS-First Strategy vs. IaaS Custom Development

Current State Problems

- **Time & Materials contracts with no deliverable accountability**: The case shows costs skyrocketing from $80,000 to nearly$59.5 million
- Building custom applications on Infrastructure-as-a-Service when SaaS solutions exist
- No standardization across departments leading to redundant development

Proposed Solution: SaaS-First with Power Platform

Predictable Pricing Model:

- E3/E5 licenses provide known monthly costs per user
- Power Platform apps scale automatically without infrastructure management
- Reduces need for specialized infrastructure teams

Speed to Market:

- Power Platform applications can be built in weeks, not years
- Citizen developers can build 80% of business applications
- Pre-built templates for common government functions

Quality & Maintainability:

- Microsoft-managed updates and security patches
- Built-in compliance features (GCDocs integration, audit trails)
- Standardized user interface reduces training costs

3. Eliminating Redundant Security Assessments

Current Waste

- **Same applications assessed repeatedly** across different agencies
- Each department conducting separate security reviews for identical SaaS platforms
- Federal organizations failed to follow procurement and security rules while creating bottlenecks

Proposed Central Assessment Framework

Single Authority Assessment:

- Create a central "Government SaaS Security Assessment" repository
- Once Microsoft 365/Power Platform is assessed for one department, it's approved for all
- Publish standardized security baselines for common platforms

Accelerated Onboarding:

- Pre-approved platforms can be deployed within 30 days
- Focus security reviews on data classification, not platform re-assessment
- Eliminate 6-12 month assessment cycles for pre-approved solutions

4. SSC Data Centre Underutilization

The Reality

- Shared Services Canada data centres are significantly underutilized
- Government continues building custom infrastructure when cloud-native solutions exist
- Operating costs remain fixed while usage is low

Strategic Rationalization

Hybrid Approach:

- Migrate commodity workloads to Microsoft 365 cloud (already security-assessed)
- Retain sensitive/classified workloads in SSC facilities
- Right-size SSC infrastructure for actual classified requirements

Cost Optimization:

- Reduce SSC operating costs by 40-60% through rightsizing
- Eliminate redundant backup and disaster recovery infrastructure (Microsoft provides this)
- Reallocate SSC expertise to govern hybrid cloud architecture

5. Accountability Framework: From Time & Materials to Deliverable-Based

Current Problem: The ArriveCAN Model

- 18% of invoices didn't have sufficient supporting documentation
- Contractors copied and pasted government requirements without adding value
- No clear accountability for deliverables

Proposed: SBIPS-Style Milestone Framework

Deliverable-Based Contracts:

- Payment tied to working software, not hours logged
- 30-60-90 day milestone deliverables
- User acceptance testing required for payment release

SaaS Procurement Model:

- Fixed monthly/annual costs for SaaS platforms
- Performance metrics tied to user adoption and business outcomes
- Built-in scalability without contract amendments

Accountability Measures:

- Project sponsors must be federal employees (not contractors)
- Clear success criteria defined before procurement
- Regular business value assessments every 90 days

6. Immediate Implementation Recommendations

Phase 1: Quick Wins (0-6 months)

1. **License Audit**: Identify all current E3/E5 holders and unused capabilities
2. **Power Platform Pilot**: Migrate 5 simple applications from custom development to Power Platform
3. **Security Assessment Consolidation**: Create central repository for pre-approved platforms

Phase 2: Systematic Transformation (6-18 months)

1. **SaaS-First Policy**: Mandate SaaS evaluation before custom development
2. **Citizen Developer Program**: Train federal employees on Power Platform
3. **Procurement Reform**: Implement deliverable-based contracting standards

Phase 3: Full Optimization (18-36 months)

1. **SSC Rationalization**: Right-size data centre infrastructure
2. **Cross-Department Standardization**: Common platforms across government
3. **Performance Metrics**: Measure cost per citizen service delivered

7. Quantified Benefits

Cost Savings Estimates

- **License Utilization**: $200M+ annually by fully leveraging existing E3/E5 capabilities
- **Reduced Custom Development**: $500M+ annually by using SaaS-first approach
- **Eliminated Redundant Security Assessments**: $50M+ annually in reduced assessment costs
- **SSC Optimization**: $100M+ annually through rightsized infrastructure

Service Delivery Improvements

- 80% faster time-to-market for new digital services
- 90% reduction in maintenance costs for business applications
- Standardized user experience across government services
- Built-in accessibility and official language compliance

8. Addressing ArriveCAN-Style Failures

Preventing Future Scandals

Transparency: SaaS platforms provide built-in audit trails and cost transparency
Accountability: Clear deliverable-based milestones prevent scope creep
Efficiency: Pre-built platforms eliminate "black box" custom development
Value: Predictable SaaS pricing prevents cost overruns

Building Public Trust

- **Open Source Components**: Where possible, use transparent, auditable solutions
- **Regular Public Reporting**: Quarterly updates on digital transformation progress
- **Citizen Feedback Integration**: Direct user feedback loops for government digital services

9. Risk Management: Legacy System Migration Strategy

Critical Legacy Application Risks

Mission-Critical System Protection:

- Phased migration approach for systems supporting essential services (EI, CPP, tax processing)
- Maintain parallel operations during transition periods
- Comprehensive rollback procedures for any failed migrations
- Legacy system maintenance contracts while modernization occurs

Risk Mitigation Framework:

- **Assessment Phase**: Catalog all mission-critical applications and dependencies
- **Pilot Testing**: Start with non-critical applications to build confidence and expertise
- **Hybrid Approach**: Maintain legacy systems while building modern interfaces using Power Platform
- **Data Integration**: Use Power Platform connectors to bridge legacy systems with modern workflows

Business Continuity:

- Zero-downtime migration strategies using API gateways
- Comprehensive disaster recovery testing before any legacy system decommissioning
- Staff retention plans for legacy system expertise during transition period

10. AI-Powered Process Automation & Service Delivery

Transformative AI Integration

Power Platform AI Capabilities:

- **AI Builder**: Pre-built AI models for document processing, forms recognition, and prediction
- **Copilot Integration**: Natural language interfaces for citizen service requests
- **Process Mining**: Automatically identify bottlenecks and optimization opportunities

Citizen Service Automation:

- **Chatbots for Common Inquiries**: 80% of routine questions automated (passport status, benefit eligibility)
- **Document Processing**: AI extraction from forms reducing manual data entry by 90%
- **Predictive Analytics**: Anticipate service demand and resource allocation needs

Internal Process Optimization:

- **Workflow Automation**: Route approvals, notifications, and escalations automatically
- **Compliance Monitoring**: AI-powered audit trail analysis and risk detection
- **Resource Optimization**: Predict and prevent system bottlenecks before they impact citizens

ROI from AI Automation

- Reduce processing times from weeks to hours for routine applications
- Free up 30-40% of administrative staff time for complex citizen interactions
- 24/7 service availability without increased staffing costs

11. Enhanced Security Framework

Zero-Trust Security Architecture

Microsoft 365 E5 Security Advantages:

- **Microsoft Defender XDR**: Integrated threat detection across all government devices and applications
- **Conditional Access**: Dynamic security policies based on user behavior and risk assessment
- **Information Protection**: Automatic classification and protection of sensitive government data

Centralized Identity Management:

- Single sign-on across all government applications reduces password-related security incidents
- Multi-factor authentication standard across all platforms
- Identity governance ensuring proper access controls during role changes

Compliance & Audit Trail

Built-in Government Compliance:

- Automated retention policies meeting government record-keeping requirements
- Immutable audit logs for all user actions and data access
- Real-time compliance monitoring and alerting for policy violations

Security Cost Savings:

- Eliminate redundant security tools across departments (estimated $100M+ annually)
- Reduce security incident response time from days to hours
- Centralized threat intelligence sharing across all government entities

12. Government-Wide Application Development Audit

Comprehensive Portfolio Review

Immediate Action Required:

- **30-Day Sprint**: Catalog all active development projects over $500K across government

- **License Compatibility Assessment**: Determine which projects could leverage existing E3/E5 capabilities
- **ROI Analysis**: Calculate potential savings from project consolidation or cancellation

Audit Findings Expected:

- 60-70% of custom development projects duplicating existing Microsoft 365 capabilities
- Multiple departments building identical functionality (citizen portals, document management, workflow systems)
- Opportunity to consolidate 200+ separate applications into Power Platform solutions

Project Rationalization Framework

Decision Matrix for Existing Projects:

1. **Continue**: Mission-critical, unique functionality not available in existing platforms
2. **Migrate**: Functionality available in Power Platform, migration feasible
3. **Terminate**: Redundant functionality, costs exceed benefits
4. **Consolidate**: Multiple departments, single shared solution possible

Immediate Cost Avoidance:

- Cancel redundant projects estimated at $300M+ in committed funding
- Redirect development resources to high-value, citizen-facing improvements
- Establish project approval gateway requiring license utilization justification

13. Central Government Open Source Repository

Federal GitHub Enterprise Strategy

"GovHub" - Internal Open Source Platform:

- Centralized repository for all government-developed code and configurations
- Peer review process ensuring code quality and security standards
- Reusable components accelerating development across departments

Power Platform Configuration Library:
Vertical-Specific Templates:

- **Grants Management**: Application processing, evaluation workflows, disbursement tracking
- **Permits & Licensing**: Application intake, review processes, approval workflows
- **Citizen Services**: Service requests, case management, status tracking
- **HR Processes**: Onboarding, performance management, leave requests
- **Financial Management**: Budget tracking, expense approval, procurement workflows

Knowledge Sharing Benefits:

- Reduce development time by 70% through template reuse
- Standardize user experience across all government digital services
- Enable rapid deployment of new services during emergencies (like COVID response)
- Cross-department collaboration and expertise sharing

Implementation Standards

Security & Access Control:

- Federal employees only, with role-based access controls
- Code scanning and security review before publication
- Integration with existing classification systems for sensitive configurations

14. Modern Identity & Access Management

Beyond Entrust: Digital Identity Revolution

Current Entrust Limitations:

- Expensive hardware tokens requiring physical replacement
- Manual provisioning delays of weeks for new employees
- No cross-agency mobility - new credentials required for each department transfer

Proposed: Decentralized Identity (DID) with Microsoft Verified ID

Seamless Cross-Agency Mobility:

- **Single Digital Identity**: Employee carries verified credentials across all government departments
- **Instant Provisioning**: New role access granted within hours, not weeks

- **Reduced Hardware Costs**: Eliminate physical tokens, leverage mobile device biometrics

Citizen Service Benefits:

- Citizens can verify their identity once for all government services
- Reduced identity verification delays for benefit applications
- Enhanced privacy through selective disclosure capabilities

Cost Savings:

- Eliminate $50M+ annually in Entrust licensing and hardware costs
- Reduce IT support tickets by 60% (password resets, token replacements)
- Enable 24/7 identity verification without manual processes

Implementation Roadmap

- **Phase 1**: Pilot with high-mobility federal workforce (consultants, shared services staff)
- **Phase 2**: Roll out to all federal employees across departments
- **Phase 3**: Extend to provincial partnerships and citizen services

15. Virtual Desktop Infrastructure (VDI) Strategy

Centralized Computing Model

Windows 365 Government Cloud:

- **Standardized Desktop Environment**: Identical experience regardless of physical location or device
- **Enhanced Security**: All data remains in government cloud, nothing stored locally
- **Simplified Device Management**: Any device becomes a secure government workstation

Cross-Agency Flexibility:

- Employees can access their full desktop environment from any government location
- Temporary assignments require no hardware provisioning
- Work-from-home capabilities without VPN complexity or security risks

Operational Benefits

Cost Optimization:

- Extend hardware lifecycles by 3-5 years (devices become thin clients)
- Centralized software licensing and patch management
- Reduced helpdesk calls through standardized environments

Business Continuity:

- Instant disaster recovery - users can access desktops from any location
- No data loss from stolen/damaged devices
- Simplified business continuity planning across all departments

16. Bi-Annual IM/IT Portfolio Governance

Mandatory Portfolio Review Consortium

Governance Structure:

- **Executive Sponsors**: DMs from major departments, CIO of Canada, SSC CEO
- **Technical Review Board**: Enterprise architects, security experts, procurement specialists
- **Citizen Advisory Panel**: Service delivery experts ensuring citizen-centric design

Review Mandate for Projects >$1M:

1. **License Utilization Justification**: Prove existing E3/E5 capabilities cannot meet requirements
2. **Inter-departmental Collaboration**: Demonstrate coordination with similar initiatives
3. **SaaS-First Assessment**: Document why SaaS solutions are inadequate
4. **Citizen Value Proposition**: Quantify improved service delivery outcomes

Project Approval Gateway

Mandatory Questions:

- "Why can't this be built using existing Power Platform capabilities?"
- "Which other departments have similar requirements for potential sharing?"
- "What SaaS alternatives were evaluated and why rejected?"
- "How does this improve citizen service delivery measurably?"

Automatic Triggers:

- Any project >$1M requires consortium review before procurement
- Projects duplicating existing functionality face automatic challenge
- Cross-departmental solutions receive priority funding and support

Accountability Measures

Performance Metrics:

- Portfolio-wide cost per citizen served
- Time-to-market for new digital services
- License utilization rates across government
- Citizen satisfaction scores for digital services

Annual Reporting:

- Public dashboard showing government digital transformation progress
- Cost savings achieved through license optimization
- Service delivery improvements quantified
- Failed project post-mortems and lessons learned

17. Benefits of Open Source Solutions Hosted on PaaS (Azure & AWS)

Why PaaS-Hosted Open Source Feels Like SaaS

- **Scalability Built-In**: Deploying open source solutions (like WordPress, Discourse, or CKAN) on Azure App Services or AWS Elastic Beanstalk allows auto-scaling, monitoring, and managed patching, much like SaaS.
- **Reduced Infrastructure Overhead**: No need to manage virtual machines or patch operating systems—PaaS handles the runtime.
- **Faster Deployment**: Pre-configured templates and container support (Docker, GitHub Actions, Azure Container Apps) reduce time-to-value.
- **Security & Compliance**: Built-in compliance certifications (SOC 2, ISO, FedRAMP) from cloud providers can be inherited.

- **Customization & Portability**: Open source projects allow deep customization and code ownership while enjoying many SaaS benefits.

Cost Efficiency

- Lower total cost of ownership (TCO) compared to traditional IaaS or on-prem hosting.
- Use of reserved instances and serverless models can further reduce long-term costs.

18. Challenges and Considerations of the Strategy

Operational Risks

- **Downtime Sensitivity**: Even on PaaS, open source workloads are not immune to outages. Application-level monitoring and failover are still needed.
- **Complex Migrations**: Migrating legacy or vendor-locked apps to PaaS-hosted open source platforms requires upfront architecture planning.

Talent & Resource Constraints

- **Open Source Expertise Gaps**: While SaaS reduces complexity, PaaS-hosted open source still requires developers and DevOps with cloud and security knowledge.
- **Dependency Management**: Projects can suffer from outdated libraries or insufficient long-term community support if governance is weak.

Procurement & Contracting Challenges

- **SBIPS Complexity**: Procuring open source-based solutions under SBIPS (Solutions-Based Informatics Professional Services) can be more complicated than SaaS:
  - Requires solution architecture and milestone-based RFPs
  - Less pricing predictability compared to SaaS subscriptions
  - Potential delays from multiple vendor handoffs and architectural disagreements

Governance Considerations

- Establishing accountability for uptime, patching, and application support is critical when using open source platforms in mission-critical settings.
- Inter-departmental coordination is required for reuse, documentation, and shared improvements.

Next Steps & Commitment Needed

Immediate Actions (Next 30 Days)

1. **Minister's Mandate**: Establish comprehensive digital-first policy framework
2. **Portfolio Audit Launch**: Begin 30-day sprint to catalog all active IT projects >$500K
3. **Consortium Formation**: Establish bi-annual review governance structure
4. **Pilot Program Selection**: Identify 5 departments for immediate Power Platform pilots

Medium-Term Implementation (90 Days)

1. **GovHub Repository**: Launch internal GitHub with initial Power Platform templates
2. **DID Pilot Program**: Begin Verified ID testing with mobile workforce
3. **VDI Strategy**: Develop Windows 365 deployment roadmap
4. **AI Integration**: Deploy first AI-powered citizen service chatbots

Long-Term Transformation (12 Months)

1. **Legacy System Migration**: Complete assessment and begin systematic modernization
2. **Cross-Agency Identity**: Full DID deployment enabling seamless mobility
3. **Portfolio Optimization**: Complete rationalization of redundant applications
4. **Citizen Service Revolution**: Deploy AI-powered, self-service government platforms

Success Metrics:

- 5-10% in annual IT cost savings within 24 months
- 80% faster service delivery for citizen applications
- 90% reduction in cross-agency employee onboarding time
- Zero major procurement scandals through transparent, accountable processes