FEDERAL GOVERNMENT · IMMIGRATION ESERVICES · HYBRID CLOUD · AUDIT-GRADE COMPLIANCE

A national immigration department's citizen-facing eServices run continuously across on-premises, AWS, and Azure — modernized release by release under audit-grade security, with one accountable delivery lead holding the cross-environment critical path.

A current, multi-year federal modernization mandate: keep always-on immigration eServices secure and compliant while migrating, automating, and re-platforming them across a hybrid cloud and on-premises estate — without an outage to the citizens who depend on them.

CLIENT **A national immigration and citizenship department (anonymized)**	ROLE **Senior Project / Technical Lead — eServices: cloud and on-premises legacy applications**	ENGAGEMENT MODEL **One accountable delivery lead integrating development, QA, DevOps, release management, and shared-services partners**
DURATION **2023 – present · multi-year, continuous modernization**	SCOPE / PLATFORMS **Citizen-facing immigration eServices · on-premises, AWS, and Azure · DEV, STE, STG, PROD**	PROGRAM SCALE **Hybrid estate · 8-member cross-environment delivery team · four controlled environments**

01 The mandate

A national immigration department delivers citizen-facing eServices that cannot stop. The applications span on-premises systems, AWS, and Azure, and must be modernized continuously — release planning, DevOps and CI/CD automation, identity and access upgrades, firewall modernization, and cloud segmentation — while remaining secure, available, and audit-grade compliant at every step. The hard constraint is not the technology; it is changing always-on public services without an interruption that would leave applicants unable to transact.

This is a sustained modernization mandate, not a one-time project: a portfolio of legacy and cloud applications, each on its own lifecycle, moved forward in coordinated releases across four controlled environments — with development, QA, DevOps, release management, and shared-services partners all converging on one schedule, under continuous security and compliance obligation.

02 The delivery context

Always-on citizen services, modernized in flight

The eServices are public-facing and operationally critical — a failed transaction is a citizen who cannot complete an immigration request. Every change therefore had to be planned, tested, and cut over without

disrupting live service, across a hybrid estate where the same application could touch on-premises, AWS, and Azure components at once. Continuity of service, not delivery convenience, set the pace.

Hybrid estate under audit-grade compliance

On-premises, AWS, and Azure environments were modernized in parallel — CI/CD automation, IAM upgrades, firewall modernization, and cloud segmentation — each carrying security and audit obligations that had to be satisfied as the work proceeded, not retrofitted afterward. Standardized governance and reporting had to hold across all four environments and every partner team simultaneously.

03 How the engagement was run

End-to-end release planning across four environments

Releases were planned and sequenced across DEV, STE, STG, and PROD so that development, QA, DevOps, release management, and shared-services partners interlocked on one timeline. Risk registers, change control, and tolerance-based escalation kept the many moving parts visible and the cutovers controlled — modernization advanced continuously without an outage to live citizen services.

Security and cloud modernization built into delivery

Identity and access management upgrades, firewall modernization, cloud segmentation, and CI/CD automation were delivered as part of the release stream rather than as separate security projects, so the estate became more secure and more automated with each release while remaining compliant and audit-ready throughout.

Governance standardized into a program-wide capability

An 8-member cross-environment team across development, QA, and DevOps was directed alongside release-management and shared-services partners under one accountable lead. Governance and reporting frameworks were standardized and then adopted program-wide — giving executives a consolidated, repeatable view of delivery health across the whole portfolio for the first time.

04 Outcome

Citizen-facing immigration eServices were modernized continuously across on-premises, AWS, and Azure — release planning, CI/CD automation, IAM and firewall modernization, and cloud segmentation delivered across DEV, STE, STG, and PROD without disrupting always-on public services. Governance and reporting frameworks were standardized and adopted program-wide, giving executives first-time portfolio-level visibility into delivery health. Commercial figures and system specifics are held confidential; the directional result is a hybrid-cloud public-service estate kept secure, compliant, and modernizing in production under a single accountable delivery lead.

DELIVERED ACROSS THE ESTATE	SCALE
Hosting estate modernized	**On-premises · AWS · Azure (hybrid)**
Controlled environments	**DEV · STE · STG · PROD**
Cross-environment delivery team	**8 members + release-management & shared-services partners**
Governance and reporting	**Standardized, then adopted program-wide**
Service continuity	**Always-on eServices modernized with no service interruption**

OUTCOME POSTURE

Always-on immigration eServices, modernized in production across on-premises, AWS, and Azure — under one accountable lead.

A current multi-year mandate: continuous, audit-grade modernization of citizen-facing public services across a hybrid estate, with governance standardized into a program-wide delivery-health view.

05 What this demonstrates

Hybrid-cloud modernization without disruption.

Modernized always-on citizen services across on-premises, AWS, and Azure — release planning, CI/CD, IAM, firewall, and segmentation — with no interruption to live public transactions.

OFFERED TODAY AS: PROGRAM LEADERSHIP

Cross-environment release leadership.

Held one release plan across DEV, STE, STG, and PROD, interlocking development, QA, DevOps, release management, and shared-services partners.

OFFERED TODAY AS: GO-LIVE READINESS LEADERSHIP

Governance that scales across a portfolio.

Standardized governance and reporting frameworks adopted program-wide, giving executives first-time portfolio-level delivery-health visibility.

OFFERED TODAY AS: PMO LEADERSHIP

Security and compliance built into delivery.

Delivered IAM upgrades, firewall modernization, and cloud segmentation inside the release stream under continuous audit-grade compliance.

OFFERED TODAY AS: SECURE DELIVERY & CLOUD MODERNIZATION

SOURCE ARTIFACTS AND DISCLOSURE

Anonymized for the public-sector and security-sensitive nature of the engagement: the department, the named citizen-facing applications, vendor product specifics, and commercial figures are withheld. Scope and team-scale figures are reported as recorded in the program's own delivery documentation. This engagement is current and ongoing.

Premium Framework Inc. is an independent IT project, program, and PMO leadership practice — founded 2011 — serving federal government, provincial agencies, public-sector institutions, and large enterprise organizations in regulated, high-stakes environments. The Delivery Track Record series presents source-substantiated program engagements, anonymized where confidentiality requires.

Talk to a delivery expert

sz@premiumframework.ca · **+1 613-600-2803** (Mon–Fri, 9–5 ET) · **calendly.com/it_delivery_management**

Tailored briefs for specific sectors or program types are available on request. Additional engagements held under confidentiality are available for discussion under NDA.