How Liberty Reclaimed Control of Its Entra ID Environment with ENow App Governance Accelerator

The Challenge

Liberty's Entra ID had become a digital ticking time bomb: hundreds of unchecked apps, expired secrets, and lurking security risks threatening a leading financial services provider. In early 2024, Liberty, with over 6,500 employees and 4,000 financial advisors, found itself grappling with a growing problem: Entra ID (formerly Azure Active Directory) application sprawl.

Despite being a regulated organization in the financial sector, covering retirement annuities, personal finance, and life insurance, Liberty's cloud identity environment had become increasingly chaotic. What began as unchecked application growth during the COVID era turned into a critical risk, with hundreds of apps, from legitimate business tools like Salesforce to personal apps like Garmin Connect and note-taking apps, living in the environment without oversight or approval. That's when Chris Bishop, a longtime consultant within Liberty's cloud security team, suspected something had to change.

Company Profile

LIBERTY
Standard Bank Group

Industry
Insurance,
Asset management

Company Size
6,500 employees

Location
Johannesburg,
South Africa

Website
www.libertyholdings.co.za

70% Ownerless:
A Tangled Web of Applications and Secrets

Chris and his team, originally focused on Active Directory and messaging, had taken on cloud responsibilities as Liberty transitioned to Microsoft 365. But the growing complexity of the environment revealed major governance, security, and business continuity blind spots: orphaned apps, over-permissioned third-party integrations, and recurring outages caused by expired secrets.

There hadn't been a structured app onboarding or offboarding program. Instead, Liberty's only app audit trails were found in random vendor docs or email threads, making it hard to identify how these applications even made it into their systems. Further in the app lifecycle, as apps became obsolete, app registrations remained in Entra, even after offboarding infrastructure. The team lacked visibility into this deprecation and lingering permissions.

"We had no idea who owned most of the applications, or even which department. We weren't consistently tracking who the owners were," Chris recalled. *"At one point, we had 774 enterprise apps in our tenant, the majority of which were ownerless or completely stale."*

Security concerns were top of mind, especially in the wake of recent breaches like the attack on Microsoft from threat actor Midnight Blizzard. Legacy applications retained dangerous permissions, including one vendor integration with the ability to impersonate users across the organization. Chris summed it up bluntly: *"We had a bit of a head-in-the-sand approach. We didn't realize the level of access some of these apps had."*

"We had no idea who owned most of the applications, or even which department. We weren't consistently tracking who the owners were."

- Chris Bishop, Liberty

Choosing AppGov for Clarity and Control

The Liberty team initially created PowerShell scripts to identify stale apps, but they took days and were inefficient for a small team juggling many Microsoft 365 and Entra responsibilities. It was clear that PowerShell would be overly tedious to use and maintain for the cleanup required. Liberty evaluated built-in Microsoft admin tools, but there was so much within the Entra admin portal that they found it lacked the ability to quickly surface problem areas and didn't provide the actionable insights and recommendations they needed.

Liberty started with the freemium version, AppGov Score, and quickly realized the scope of the problem. "Our initial score was 47%, and we kind of just looked at each other and were like, oh boy, what are we doing wrong?" That number represented hundreds of apps with expired secrets, risky permissions, or no clear owner.

Chris knew they needed to move fast, but also strategically.

The Cleanup Strategy: Learning by Doing

With App Governance Accelerator quickly implemented, Liberty immediately gains visibility and clarity on ownership, permissions, and lifecycle status, enabling them to take meaningful action to reduce risk in their environment. Chris noted, "The onboarding of AppGov was rather easy. I accepted the consent and used their documentation to limit the scope and permissions to only specific users. Not only was it easy, but it's reassuring to know ENow is practicing what they preach when it comes to appropriately securing and governing apps, including their own."

The Liberty team approached the cleanup process in stages. They quickly realized that many cleanup roads led to Ownership at its source. Due to the dispersed nature of App Ownership at this point, they needed to crowdsource some elements of the cleanup process. They exported a list of all ownerless apps from AppGov, compiled it into a SharePoint Excel sheet, and worked department by department, working closely with Information Security Officers and business users to track down responsible parties.

This shift towards known owners unlocked momentum. Within six months, Liberty had reduced its app inventory from 774 to 221 enterprise apps and deleted nearly 300 unnecessary registrations. Their AppGov score climbed from 47% to a peak of 70%, as they refined processes and tackled new findings that AppGov swiftly uncovered.

> **"** The onboarding of AppGov was rather easy. I accepted the consent and used their documentation to limit the scope and permissions to only specific users. **"**

Chris Bishop
Consultant - Exchange, Microsoft 365 & Active Directory at Liberty

Tangible Gains in Time, Security, and Culture

App Governance Accelerator's real-time insights and direct links to the Entra admin blade saved countless hours. "*I don't even think you can count how much time it saved; it's been a lot,*" said Chris. "*If we had to run this project manually ourselves, we would've been looking at one to two years. With AppGov, we got most of the initial cleanup work done in six months.*"

"*When we started looking at secrets, there were probably over 100 secrets that had expired and needed to be cleaned up,*" shared Chris. Before AppGov, expired secrets led to critical business disruptions, triggering 2 AM calls from staff. Now they're proactively flagged. According to Chris, a relief to the team, those fire drills are gone.

Secrets management also improved: "*Now we can push ownership to where it belongs, instead of the cloud security team managing every secret manually.*" The Professional edition of App Governance Accelerator will trigger notifications when secrets and certs are expiring, prompting proactive action to avoid business disruptions.

The benefits weren't just technical. AppGov helped elevate security conversations across leadership. "*The CISO and department heads were pleased with the work on secrets and risky apps. There's more visibility and trust now. It's really helped open our eyes.*" As a South African financial services provider, Liberty bolstered its compliance posture, ensuring audit-readiness and robust data protection with a governed Entra ID environment.

Liberty's App Governance Accelerator Results in Just 6 Months

Metric	Before AppGov	Using AppGov
Total Enterprise Apps	774	221
Ownerless Apps	70%+	14% and shrinking
Expired Secrets	Dozens triggering outages	Proactively managed
AppGov Score	47%	70% and increasing
Time Savings	Estimated 1–2 years of manual work	Reduced to 6 months
Business Disruption Incidents	2-3 times per month (due to expired secrets)	Minimal since implementation

Looking Ahead

Liberty continues on its app governance journey. They're on track to assign owners to the remaining 14% of ownerless apps, renew expired secrets of apps that are still required and used, and develop a formal onboarding/offboarding process to ensure strong governance practices continue. Beyond cleanup, ENow App Governance Accelerator positions Liberty to securely scale their Microsoft 365 adoption, integrate future third-party SaaS apps, and confidently embrace new cloud capabilities without repeating past sprawl.

"*AppGov has exposed where the gaps are and has simplified the remediation process. App Governance Accelerator has been a catalyst, empowering us to get in the best possible position to stay ahead of application-related risks,*" Chris noted.

App Governance Advice for Others

When asked what advice he'd offer to other IT teams, Chris didn't hesitate, "*Find a tool that can help you. Trying to manage this manually was next to impossible. AppGov makes it much easier.*" He added, "*Start with app ownership; it's the foundation for governance. Tools like AppGov turn a daunting task into a manageable win.*"

ENow App Governance Accelerator

See Clearly

Uncover every app in your Entra ID tenant, including stale and over-permissioned apps, with immediate visibility into risks that manual methods miss.

Fix What's Broken

Take action fast with guided workflows: clean up expired secrets and eliminate unnecessary registrations that put your organization at risk.

Establish Control

Establish structured onboarding, offboarding, and ownership processes so apps are managed consistently across teams, improving compliance and audit readiness.

Stay Ahead

Stay ahead with proactive alerts and real-time insights into secrets, permissions, and new app activity to prevent outages and reduce business disruption.

Ready to start your App Governance journey? <u>Get your free AppGov Score today</u>!

About ENow Software

ENow protects and optimizes Microsoft Copilot, Microsoft 365, and Microsoft Entra ID, by empowering the Modern Workplace Leader with a single platform that drives outcomes for Adoption, Governance, Monitoring, License Optimization, and Entra ID Application Governance.