

Nationwide Building Society

Privileged Access Management Transformation

Copyright© 2024 Accenture. All rights reserved.

Nationwide Building Society

CLIENT CONTEXT

Nationwide is the largest building society in the world, and a large financial services organization in the UK providing retail banking services to over 17 million customers in the UK. Accenture is the Security partner at Nationwide, and has been involved in delivering multiple engagements in the Security space over the years.

THE CHALLENGE



IAM tried twice and failed, third
 IAM project initiative at risk



 Inexperienced project, architecture and advisory teams with no real exposure to IAM challenges



 A highly customized IAM platform developed by incumbent supplier unable to scale to the demands



 Growing backlogs and skipped milestone commitments to the board

THE JOURNEY



Successfully rolling out a re-designed IAG
platform capable of rapidly on-boarding and
governing access across hundreds of
applications by leveraging Accenture
accelerators, Design patterns, DevOps and
Automation



 Setting up an industrialized IAM factory to onboard high risk and high request volume applications to provide efficient governance



 Maximizing investment on IAG platform by automating manually managed governance processes using the IAG capabilities thereby reducing cost to operate

KEY IMPACT

- With Accenture as the driving force, the society successfully rolled out the SailPoint IIQ platform to workforce users in October 2018 and prioritized applications that would yield the highest ROI.
- With the subsequent roll-out of automated access re-certification, Preventative and Detective Toxic combination capabilities the security and governance posture of the society has significantly improved.
- Accenture Security has helped the society deliver a true business enabler and to successfully manage audit concerns with an IAG platform protecting and serving the business.

Nationwide Identity and Privileged Access Transformation Journey

We've been helping Nationwide successfully roll-out the Workforce Identity and Privileged Access solutions (SailPoint IIQ + CyberArk)

Scope

- Identity transformation
- Identity run services
- Security Architecture

Teams:

Security Architects: 4 Transformation: 14 Support Specialists: 5

Key skills:

SailPoint Identity IQ, CyberArk, API management, SCIM, Microsoft SQL Server Integration and Reporting services, Active Directory, ServiceNow, DevOps, IAM Architecture

Key capabilities delivered:

- **Automated Identity and Privileged controls**
 - Joiner, Mover & Leavers
 - Access Request & approvals
 - **Access Request Recertifications**
 - Privileged access onboarding and monitoring
 - Additional native controls
- 440+ Tier1 & 2 systems onboarded to CvberArk
- 105+ applications onboarded to SailPoint
- Scalable Cloud RBAC Model for AWS cloud roles live in production

Key business outcome:

- 140+ internal and external audit events
- Paper based forms translated to automated request in IIQ
- Average time to grant access reduced from 12 days to 30 mins
- Helpdesk calls reduced from 200 to 20 calls per day
- Recertification controls for 300+ AD application and 70+ Non-AD applications
- **50%** cost reduction to re-certify
- 60% Op-ex savings driven through automation
- Full transition of PAM & IGA application onboarding to NBS insourced teams

IGA Journey



Successfully roll-out workforce identity platform along with automated access,



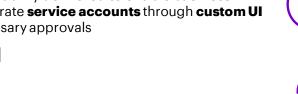
controls, governance and reporting Achieved audit compliance



2020

ADGM capability controls for continued assurance and address PRA audit action

NOAM capability delivered to enable business teams operate service accounts through custom UI with necessary approvals



2022

Ongoing initiatives:

- Native change detection phase 2
- Retail flexible roles
- **Attack surface management**
- **Zero Trust**
- **Security operations automation**





2017

NBS Security and Resilience org initiatives:

- **IGA** programme
- **PAM** programme

Decision to move from earlier supplier and partner with Accenture



Daily batch process re-designed to reduce the process execution time by 60%

Native change detection capability to detect and respond to malicious activity outside of SailPoint IIQ



NOAM enhancements

Integration with Cloud **COE(Cloud RBAC) roles** for automated cloud role request



Least Privileged Access Management

Application Onboarding: Federated Access Control

Native Change Detection

















Application on-boarding