Identity & Access Management

Quarterly Assessment & Governance Summary Report –IT/Sales& Marketing/Finance managed Asset(s) Q2 -2025

**Shape

Description automatically generated with medium confidence**

**Document History**

|  |  |
| --- | --- |
| Date | 16-Jul-2025 |
| Title | IT Managed Asset(s) |
| Quarter | Q2 |
| Version History | v1.0 |
| Conducted By | Infosec |
| Author | Garima Bhatt |
| Reviewer | Saravanan Sankaran |

**Purpose**

Netradyne’s Identity & Access management assessment is an important control activity required for internal and external IAM audits, helping to minimize threats and provide assurance that the right people have the right access to critical systems and infrastructure. This procedure details process steps and provides control owner guidance for access reviews.

**Benefits to the organization:**

* Reduces security risk.
* Identifies dormant and/or disabled accounts.
* Ensures only required team members have access to a system.
* Validates users who have changed roles have not retained access no longer relevant.
* Ensures terminated team members no longer can access company systems.
* Ensures role-based access control should be implemented in each assets/application.
* Ensure MFA should be enabled on each asset.

**Scope**

Evaluate access to the Higher Risk/Higher Priority applications with the system (Asset) owner and review the roles used by the department. E.g., NetSuite Access, the key question to answer is, “Should the department have those roles?” At this point the system (Asset) owner can remove users who should not have access to their application(s).

Remove departments and users who should not have any access to the respective system (Asset)

Eliminate users from applications who should no longer have access (e.g., the position they are in now no longer requires access to the application).

Meet with the functional owners and leads to review the approved applications / systems.

Infosec IAM will manage the governance process and ensure compliance of the Access Control Matrix with all the stakeholders. Infosec to conduct internal IAM assessment quarterly to review and report compliance to leadership.

**Roles & Responsibilities:**

| **Role** | **Responsibility** |
| --- | --- |
| Infosec Team:  Garima Bhatt (IAM)  Saravanan Sankaran (CISO) | \* Execution of entitlement reviews  \* Execution of terminated user access reviews  \* Creation of observations and oversight of remediation activities for any identified findings |
| Asset(s): [IT\_Managed\_Applications.xlsx](https://netorg726775.sharepoint.com/:x:/r/sites/InfosecInternal/_layouts/15/Doc.aspx?action=edit&sourcedoc=%7B3466110b-25ac-463c-819b-3a49dd09c23d%7D&wdOrigin=TEAMS-ELECTRON.teamsSdk.openFilePreview&wdExp=TEAMS-CONTROL&web=1&wdLOR=c922E710F-DAF9-4544-8E8E-34DCE81900E2&cid=d58cecb8-ec4b-457f-9d40-fd63796ecad7)  Asset/System/Support Owners  Asset Managed By: IT, Sales & Marketing, Finance | \* Validation of privileged entitlements  \* Validation of user entitlements  \* Timely evidence supports  \* Execution of remediation plans for identified observations  \* Support validation of privileged entitlements  \* Support validation of user entitlements |
| Security Assurance Management | Responsible for approving significant changes and exceptions to this procedure |

## Access Review Procedure

* 1. Requested the Identity & Access management data from the targeted functional areas in the [*IAM tracker*](https://netorg726775.sharepoint.com/:x:/s/InfoSecDocumentGovernanceRepository/EVR0WcCOK6BGgmOGybMHvXIBndTJg744SkZxz_ycYi4EfA?CID=34BE98C6-D6BF-49A7-B72E-F8EFA64EDF53&wdLOR=c048E3495-FE40-49E5-9C32-F0FB83423621) aligned with [Access Control Matrix](https://netorg726775.sharepoint.com/:x:/r/sites/IT/_layouts/15/Doc.aspx?sourcedoc=%7BB9F6587A-BE8C-430D-A5D9-88E9ECF307F5%7D&file=Netradyne-Access_Control_matrix.xlsx&action=default&mobileredirect=true&cid=8cd8b91d-959d-4709-9740-6b6dce79383c) which includes the following access list.

Access list for review in the IAM tracker:

* Asset Criticality (Impact to customer / No impact to customer)
* Environment (Production / Non - production)
* Roles
* Access Types (Privilege / Non privilege)
* Permanent access / Temporary access
* Access expiry time
* Username, UPN, User ID, email
* User Status (Employee/ Contractor/ Vendor)
* Account Status (Active / Inactive)
* MFA Status (Enabled / Disabled)
* Generic Account / Unique account

2. Access reviews was done after collating the data internally and shared the findings with the respective departments.

4. Access validation sessions were conducted with the respective Asset owner and administrators.

5. Identifies the gaps and shared Infosec recommendations

**Privilege Access Details**

[IAM Governance Ageing Report.xlsx](https://netorg726775.sharepoint.com/:x:/r/sites/InfoSecDocumentGovernanceRepository/_layouts/15/Doc.aspx?sourcedoc=%7B2C827087-8219-4ED0-BF3F-DF2D4ADD4C39%7D&file=IAM%20Governance%20Ageing%20Report-2025.xlsx&action=default&mobileredirect=true)

**Identified Gaps:**

[IT IAM Report Q2’25.xlsx](https://netorg726775.sharepoint.com/:x:/r/sites/InfoSecDocumentGovernanceRepository/_layouts/15/Doc2.aspx?action=edit&sourcedoc=%7B5ad73ac9-4ba3-4a3f-bbea-d8b242277be5%7D&wdOrigin=TEAMS-MAGLEV.teamsSdk_ns.rwc&wdExp=TEAMS-TREATMENT&wdhostclicktime=1752559828245&web=1)

**Conclusion:**

Overall, 10 High, 12 Medium & 2 Low gaps were identified as part of IAM Quarterly Assessment & Governance IT managed application(s) in Q2’25.

|  |  |
| --- | --- |
| High | 10 |
| Medium | 12 |
| Low | 2 |

**Note:** The assigned Priority and Impact levels (High, Medium, or Low) are determined based on the nature of the findings. Examples include:

* Excessive administrative privileges
* No periodic access reviews conducted
* Inactive admin accounts (no login activity for ≥90 days)
* Shared or generic admin accounts
* Privileged access without Multi-Factor Authentication (MFA)
* Lack of session timeout policies
* Broad access granted without business justification
* Privileged roles assigned outside of RBAC standards

These factors help assess the risk and urgency of remediation.

Recommendations has been shared and requested the stakeholders to close it by the given ETA.

**Summary Table**

