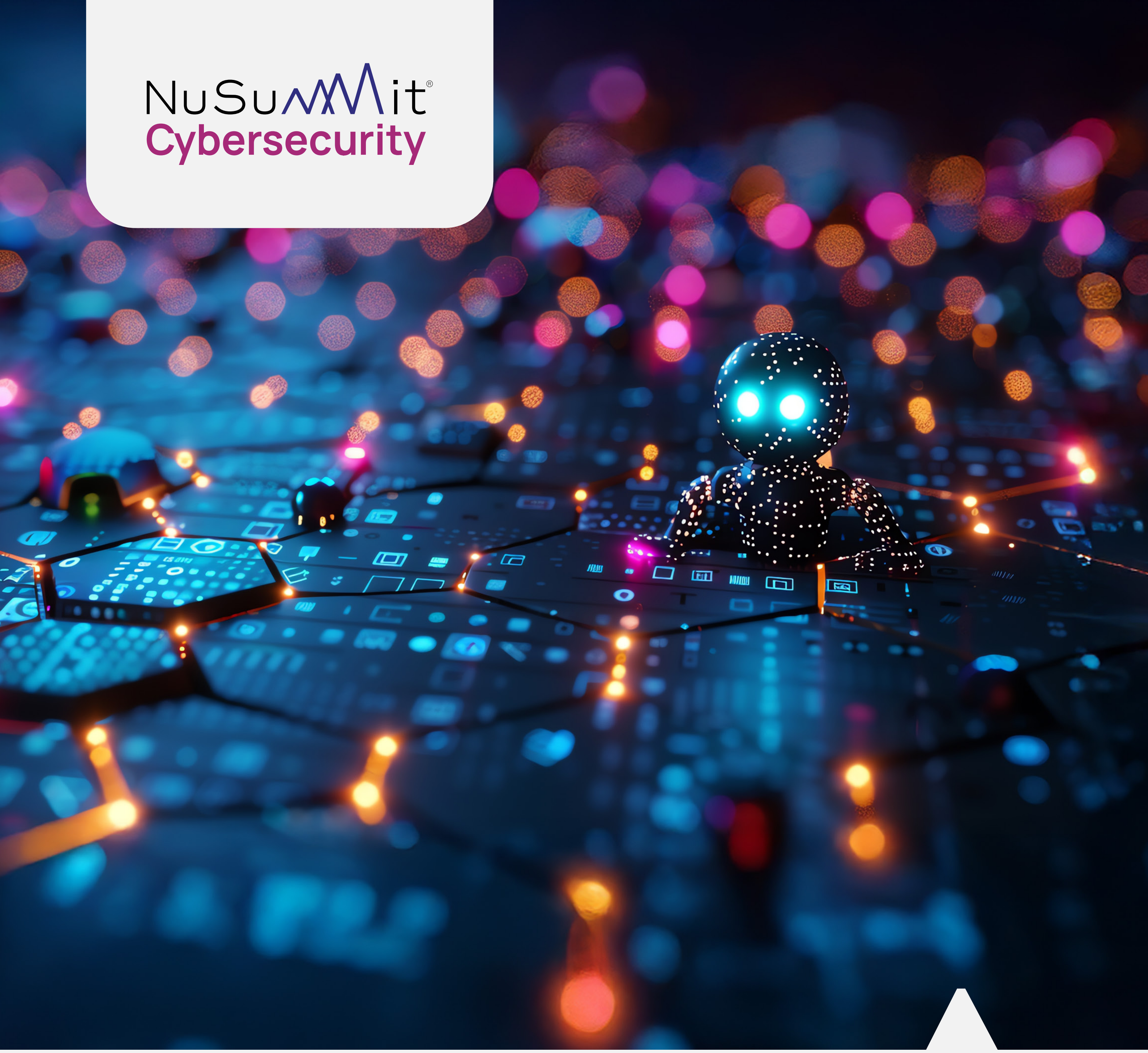
NuSummit Cybersecurity



WHITEPAPER

IRDAI Information and Cybersecurity Guidelines

IDENTITY AND ACCESS MANAGEMENT

cybersecurity.nusummit.com

Table of Contents

Policy Compliance Details

09

Access Control

3.1 User Identification and Accounts

3.2 Group/Generic User IDs

3.3 User-Id Creation and Maintenance

3.4 User Authorization

3.5 Privileged User Accounts

3.6 Secure Log-On

3.6.1 Review Of Access Rights

3.7 Remote Access

3.8 Compliance and Audit

Bring Your Own Device (BYOD Policy)

3.7.2.1 Device Security

Network Security

3.1.2 Types Of Connectivity

Monitoring, Logging And Assessment

3.5 User Activity Monitoring

3.3.2 Application Access & Activity

Cloud Security Policy

3.4.1 Authentication

Introduction

In India's dynamic insurance market, fraud is a growing concern impacting real lives and savings. Insurance companies are intensifying fraud prevention efforts to protect their profits and safeguard millions of families relying on insurance. Fraud undermines trust, inflates policy costs, and doubts genuine claims. Preventing fraud is about honoring a promise to policyholders. It ensures that claimants can focus on recovery, not on the legitimacy of their claims during health crises or unexpected losses. Insurance companies must tackle fraud head-on, building trust one policy at a time. In India's diverse market, this trust is essential for a secure, thriving insurance sector that truly serves its people.

Regulatory Framework and the IRDAI's Initiatives

The Insurance Regulatory and Development Authority of India (IRDAI) is the primary regulatory body overseeing the insurance sector in India. It has introduced comprehensive guidelines to combat insurance fraud effectively. These guidelines include key legislation such as the Insurance Act of 1938 (as amended), the IRDA Act of 1999, and the Prevention of Money Laundering Act of 2002. These regulations collectively provide a robust legal framework to tackle insurance fraud, outlining the responsibilities and obligations of insurance companies.

In addition, IRDAI has reinforced this legal framework with its Information and Cyber Security Guidelines, Version 1, issued in April 2023. These guidelines mandate effective cybersecurity frameworks, conduct regular risk assessments, develop incident response plans, and ensure board-level oversight of cybersecurity measures. Compliance with these regulations allows insurers to enhance fraud prevention capabilities and demonstrate commitment to safeguarding sensitive customer data. This proactive approach to security and compliance positions insurers to build trust, mitigate risks, and thrive in India's dynamic insurance market.

NuSummit Cybersecurity IAM Approach

NuSummit Cybersecurity excels in delivering cutting-edge Identity and Access Management (IAM) solutions for any scenario. Our expertise cuts through the complexity of multi-faceted technological scenarios, offering a comprehensive approach from strategic planning to ongoing administration.

This document is a comprehensive study offering detailed insights into NuSummit Cybersecurity's proposed IAM solution's adherence to the IRDAI Information and Cyber Security Guidelines.

Summary - IRDAI Policies and IAM Solution Compliance

Policy No.	Policy Name	Section No.	Section Name	Sub Section No.	IAM Solution Compliance
1.3	Principles and Objectives	1.3	Principles and Objectives	NA	Yes
2.2	Asset Management	3.2.2.3	Authorization Inventory	3	Yes
2.3	Access Control	3.1	User Identification and Accounts	1, 2, 3	Yes
2.3	Access Control	3.2	Group/ Generic User IDs	1, 2	Yes
2.3		1.3	User-ID Creation and Maintenance	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	Yes
2.3	Access Control	3.4	User Authorization	1, 2, 6, 7, 8, 9, 12, 13, 14	Yes
2.3	Access Control	3.5	Privileged User Accounts	3, 4, 11	Yes
2.3	Access Control	3.6	Secure Log-On	1, 2, 3, 4, 5, 6, 7, 8	Yes
2.3	Access Control	3.6.1	Review Of Access Rights	1, 2, 3, 4	Yes
2.3	Access Control	3.7	Remote Access	2, 5	Yes

Policy No.	Policy Name	Section No.	Section Name	Sub Section No.	IAM Solution Compliance
2.3	Access Control	3.8	Compliance and Audit	2, 3, 4, 8	Yes
2.8	Bring Your Own Device (BYOD) Policy	3.7.2.1	Device Security	2	Yes
2.11	Network Security	3.1.2	Types Of Connectivity	6	Yes
2.16	Monitoring, Logging and Assessment	3.5	User Activity Monitoring	1, 2, 3	Yes
2.16	Monitoring, Logging and Assessment	3.7.2.1	Application Access & Activity	6	Yes
2.3	Cloud Security Policy	3.4.1	Authentication	NA	Yes
2.22	Work From Remote Location	3.1	Framework	1	Yes
2.22	Work From Remote Location	3.2	Network Security	2	Yes
2.22	Work From Remote Location	3.3	Data Management	1	Yes
2.22	Work From Remote Location	3.4	Human Resource Security	3	Yes
2.3	Dealing Room Operations	3.3	Data Security	2	Yes

Policy Compliance Details

This section maps our IAM solution approach against the corresponding IRDAI policies that include the following:

- Principles and Objectives
- Asset Management
- Access Control
- Device Security
- Network Security
- Monitoring, Logging and Assessment
- Cloud Security
- Remote Access
- Dealing Room Operations

Principles and Objectives

This section maps the IAM capability that adheres to the IRDAI core principles and objectives designed to enhance the security posture of insurance companies in India.

Section : Not applicable

Sub Sec.	Compliance requirements	How we can help?
2	User Authentication and Authorization - All Users must be uniquely identifiable with access permissions specifically and individually authorized based on their business needs. User access methods should stress strong authentication, appropriate authorization and reliable audit-ability.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, role-based access controls, periodic access reviews, Single Sign-On, and strong authentication using various MFA options, including password-less and FIDO2-based authentication.

Asset Management

This section maps the IAM capability to the Asset Management section of the IRDAI Information and Cyber Security Guidelines, which focuses on the comprehensive management of information assets within insurance companies.

Section : 3.2.2.3 Authorization inventory

Sub Sec.	Compliance requirements	How we can help?
3	For non-organization-owned assets, the authorization record shall consist of parameters used for two factor authentication such as username and password, token ID or biometric record.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options, including password-less and FIDO2-based authentication.

Access Control

This section maps the IAM capability that adheres to the Access Control section of the IRDAI Information and Cybersecurity Guidelines and emphasizes the critical need for stringent access management to protect sensitive information within insurance companies. It outlines the principles and practices for ensuring that access to information assets is restricted to authorized personnel only based on their roles and responsibilities. By enforcing robust access control measures, organizations can prevent unauthorized access, reduce the risk of data breaches, and maintain the confidentiality and integrity of their information systems.

Section : 3.2.2.3 Authorization Inventory

Sub Sec.	Compliance requirements	How we can help?
1	A User-ID or account shall be assigned to each individual to authorize a defined level of access to information assets and shall be protected by authenticating the user to the User-ID upon requesting access.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, Single Sign-On, and strong authentication using various MFA options, including password-less and FIDO2-based authentication.
2	Each User- ID or account on organization's informaton systems shall uniquely identify only one user or process. Every individual user shall be accountable for all actions associated with his /her User-ID. User-IDs shall not be utilized by anyone other than the individuals to whom they have been issued. Users shall not allow others to perform any activity with their User-IDs. Similarly, users shall be forbidden from performing any activity with User IDs belonging to other users.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, Single Sign-On, and strong authentication using various MFA options, including password-less and FIDO2-based authentication.

3	Where it is not possible to implement individual User- IDs and passwords within the system due to technology limitations or process design, alternative solutions for restricting and auditing access privileges shall be evaluated for feasibility and shall be implemented.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, periodic user access reviews, and RPA-based integrations.

Section : 3.2 Group/ Generic User IDs

Sub Sec.	Compliance requirements	How we can help?
1	The use of generic and group User-IDs shall be avoided wherever possible. Wherever there is no alternative available / it is absolutely essential a group account shall be used; however, it shall follow the Exception grant and risk assessment methodology requiring the prior authorization of the appropriate authorities and clear accountability to one individual (Group ID owner) shall be established. The use of Group-ID shall be short term in nature having an expiration date.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, Single Sign-On, and strong authentication using various MFA options, including password-less and FIDO2-based authentication.
2	Generic User-IDs shall not be created unless necessitated by technology limitations or under business exigencies. An owner shall be identified for every generic User-ID created and the owner shall be held accountable for all actions associated with	The proposed IAM solution will address the policy requirement by implementing non-human/machine-identity management, periodic user access, and account ownership reviews.

	the generic User-ID. Where it is required for a generic User-ID to be shared between multiple individuals, alternative solutions for assigning and ascertaining accountability at all times shall be evaluated for feasibility and shall be implemented.	

Section : 3.3 User-ID creation and Maintenance

Sub Sec.	Compliance requirements	How we can help?
1	User-IDs shall be non-transferrable, and individuals shall not have multiple accounts within the same computing environment.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management and periodic user access reviews.
2	Access to organization's environment such as the network shall be granted only upon intimation received from HR. All users shall be granted access to the information systems and services through a formal user registration process that shall include the approval of access rights from authorized personnel before granting access.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, access request and approval flows, role-based access control, and periodic user access reviews.
3	All users shall follow a formal de-registration process for revocation of access to all information systems and services which shall include automated or timely intimation and revocation	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, including an automated joiner-mover-leaver process.

	rights. Intimation for revocation of access rights shall come from HR. A confirmation of the access revocation shall be sent to HR as a part of the exit clearance process.	
4	Levels of access granted to all Users shall enforce segregation of duties and adhere to the “need to know” principle. Where segregation of duties cannot be enforced by logical access controls, other non-IT- related controls shall be implemented.	The proposed IAM solution will address the policy requirement by implementing preventive and detective Segregation of Duty checks, assisted by automated user life cycle management, access request policies, and periodic user access reviews.
5	An initial password shall be provided to the users securely during the user creation process and the system shall be configured to force the users to change the initial password immediately after the first logon.	The proposed IAM solution will address the policy requirement by implementing an automated user life cycle management process.
6	Appropriate procedures shall be put in place for storing and management of administrative passwords for critical information systems. All user passwords shall be encrypted while in transmission and storage.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management and self-service password management processes.
7	The password requirements for all user accounts shall follow the password standards as defined in the Password Standard. Any exceptions to the password standard shall follow the Exception grant and risk assessment methodology requiring the prior authorization of the appropriate authorities and counter measures shall be implemented to mitigate the resulting risk.	The proposed IAM solution will address the policy requirement by implementing a consistent password policy across all users and applications.

8	Users shall be required to change their passwords at the first log-on and change their passwords once in 45 days.	The proposed IAM solution will address the policy requirement by implementing access management (SSO, MFA) and a strong, consistent password policy across all users and applications.
9	A record of previously used passwords shall be maintained to prevent re-use. Further, password files shall be stored separately from application system data.	The proposed IAM solution will address the policy requirement by implementing a strong and consistent password policy across all users and applications.
10	The respective Department Heads for all individual users or user groups shall review the access rights or privileges assigned to the corresponding system periodically. Any exceptions noted shall be addressed at the earliest.	The proposed IAM solution will address the policy requirement by implementing automated account management for PAM systems and periodic privileged user access review campaigns.
11	The department heads shall maintain a central record of access rights granted to a user-id to access information systems and services.	The proposed IAM solution will address the policy requirement by implementing a unified identity repository with a single pane of glass view of all assigned accesses across users and applications.
12	In case of transfer of an employee from one function to another, access rights of the user shall be revoked for previous functional role and access need to be provided for new functional role.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, including an automated joiner-mover-leaver process utilizing role-based access control.

Section : 3.4 User Authorization

Sub Sec.	Compliance requirements	How we can help?
1	Users shall be authorized on organizations information systems at the following levels: • Physical access • Network • Infrastructure • Endpoints • Applications • Cloud (where applicable)	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.
2	User authorization mechanisms at each level shall be independent of authorization at a previous or subsequent level for example, applications shall perform assessment of user authorization request independent of the operating system authorization process.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.
6	Access to all endpoints and applications shall be permitted only after authorization of the user credentials by the host operating system or the application itself.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.
7	Applications shall support integration with the enterprise identity management system.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.

8	If the authorization request comes from a organization owned asset (device/network), single factor authentication will suffice. In case the authorization request comes from a non-Organization asset (device/network) two-factor authentication will be mandatory.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong and conditional authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.
9	Applications hosted on the Cloud shall accept a user authorization record validated by a organization-owned authorization service or require two factor authorization as stated in (6) above.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong and conditional authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.
12	Users shall be required to re-authenticate themselves after a specific period of inactivity.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong and conditional authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.
13	Organization shall establish process for granting access based on emergency.	The proposed IAM solution will address the policy requirement by implementing emergency access provisioning and de-provisioning flows.
14	Organization shall establish methods to prevent unauthorized access by other groups into individual files and department-shared files.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management leveraging role-based or attribute-based access control and segregation of duties.

Section : 3.5 Privileged User Accounts

Sub Sec.	Compliance requirements	How we can help?
3	Privileged user accounts shall be limited to individuals with specific business justification for this level of access. Such access shall only be granted upon authorization from appropriate personnel.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management and periodic user access reviews for privileged users and accesses.
4	Privileges shall be allocated to individuals on a 'need to have' basis in strict adherence to the authorization process for privilege access.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management and periodic user access reviews for privileged users and accesses.
11	An authorization process and a record of all privileges allocated shall be maintained.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management and periodic user access reviews for privileged users and accesses.

Section : 3.6 Secure Log-on

Sub Sec.	Compliance requirements	How we can help?
3	The Log-on process shall not provide any information that would aid an unauthorized user to successfully Log-on.	The proposed IAM solution will address the policy requirement by implementing appropriate password policies, authentication flows, Single Sign-on, and strong authentication using various MFA options, including

		password-less and FIDO2-based authentication for application and cloud-platform access.
2	Log-on data shall only be validated after it has all been entered.	The proposed IAM solution will address the policy requirement by implementing an appropriate password policy, authentication flow, Single Sign- And strong authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.
2	The log-on process shall not reveal which part of the log on data is valid or invalid.	The proposed IAM solution will address the policy requirement by implementing an appropriate password policy, authentication flow, Single Sign- And strong authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.
4	Account lockout shall be enforced by the log-on process after the retry limit is reached.	The proposed IAM solution will address the policy requirement by implementing an appropriate password policy, authentication flow, Single Sign- And strong authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.

5	Log-on process shall display a general notice warning that the computer should only be accessed by authorized user.	The proposed IAM solution will address the policy requirement by implementing an appropriate password policy, authentication flow, Single Sign- And strong authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.
6	Log of unsuccessful and successful attempts shall be maintained.	The proposed IAM solution will address the policy requirement by implementing an appropriate password policy, authentication flow, Single Sign- And strong authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.
7	The log-on process shall not transmit passwords in clear text over a network.	The proposed IAM solution will address the policy requirement by implementing an appropriate password policy, authentication flow, Single Sign- And strong authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.

8	The log-on process shall terminate inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organization’s security management or on mobile devices.	The proposed IAM solution will address the policy requirement by implementing an appropriate password policy, authentication flow, Single Sign- And strong authentication using various MFA options, including password-less and FIDO2-based authentication for application and cloud-platform access.

Section : 3.6.1 Review of Access Rights

Sub Sec.	Compliance requirements	How we can help?
1	User access rights shall be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management and periodic user access reviews for all the users, applications, and accesses.
2	User access rights shall be reviewed and re-allocated when moving from one role to another within the same organization.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management and periodic user access reviews for all the users, applications, and accesses.
3	Authorizations for privileged access rights shall be reviewed at more frequent intervals and changes to privileged accounts shall be logged for periodic review.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management and periodic privileged user access reviews for all the privileged users, privileged applications, and elevated accesses.

4	Privilege allocations shall be checked at regular intervals to ensure that unauthorized privileges have not been obtained.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management and periodic privileged user access reviews for all the privileged users, privileged applications, and elevated accesses.

Section : 3.7 Remote Access

Sub Sec.	Compliance requirements	How we can help?
1	Remote access request for third party vendor/consultant shall be raised by the organization employee responsible for the vendor /consultant engagement along with proper business justification. The request needs to be approved by sponsoring functional manager, Head IT and Group CISO. If access is provided from non organization endpoints an exception shall be taken in this regards Head-IT and Group CISO.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, non-employee/third-party risk management, and periodic user access reviews for all the users, applications, and accesses.
2	An expiration of not more than 15 days or lesser shall be placed on all third party user-IDs unless appropriate approval is given. Expiration of IDs will occur in the authenticating database. After the expiration, third parties who wish to continue working for organization should obtain approval in order to regain the User-ID.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, non-employee/third-party risk management, and periodic user access reviews for all the users, applications, and accesses.

Section : 3.8 Compliance and Audit

Sub Sec.	Compliance requirements	How we can help?
2	Remote Access System Owners shall maintain evidence of all requests for granting remote access.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, non-employee/ third-party risk management, access requests, and approval flow.
3	All notifications for initiating the revoking of remote access.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, non-employee/ third-party risk management, access requests, and approval flow.
4	All evidence for granting, revoking, or changing remote access privileges shall be maintained in a repository such as Change Management System.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, non-employee/ third-party risk management, access requests, and approval flow.
5	On a monthly basis the system owner's shall ensure that the accounts active within the Remote access solutions are accurate. All discrepancies shall be resolved quickly.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management, non-employee/ third-party risk management, access request and approval flow, and periodic user access reviews.

Bring Your Own Device (BYOD)

This section maps the IAM capability that adheres to the IRDAI Information and Cyber Security Guidelines related to the policies and controls necessary for managing personal devices used for work purposes within insurance companies. By implementing robust BYOD policies, organizations can mitigate risks associated with personal devices, ensure data security, and maintain compliance with regulatory requirements.

Section : 3.7.2.1 Device Security

Sub Sec.	Compliance requirements	How we can help?
1	Access to organization applications data: As defined in the 'Security Policies: Access control' , access to all organization application and/or data will be based on two factor authentication.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options, including password-less and FIDO2-based authentication.

Network Security

This section maps the IAM capability that adheres to the IRDAI Information and Cyber Security Guidelines, outlining the essential measures and practices for protecting the network infrastructure of insurance companies.

Section : 3.1.2 Types Of Connectivity

Sub Sec.	Compliance requirements	How we can help?
1	Any connect on to organization's IT assets classified as business transaction systems and high severity systems from outside organization-owned or controlled network (ex. remote connections), shall require two factor authentication as defined in the access control policy and compliance check validates the device connecting.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options, including password-less and FIDO2-based authentication.

Monitoring, Logging, and Assessment

This policy maps the IAM capability that adheres to the IRDAI Information and Cyber Security Guidelines that highlight the critical processes for continuously overseeing and evaluating the security of information systems within insurance companies.

Section : 3.5 User Activity Monitoring

Sub Sec.	Compliance requirements	How we can help?
1	User accounts shall be monitored regularly to detect any unwanted privileges, orphan accounts, and dormant accounts. Any accounts detected in violation of organization's policies shall be suspended or terminated.	The proposed IAM solution will address the policy requirement by implementing a unified identity repository, automated user life cycle management, and periodic user access reviews.
2	Redundant/dormant user-ids shall not be issued to other users.	The proposed IAM solution will address the policy requirement by implementing a unified identity repository, automated user life cycle management, and periodic user access reviews.
3	A periodic account review shall be conducted and respective managers shall be required to match the current user rights with the business requirements.	The proposed IAM solution will address the policy requirement by implementing a unified identity repository, automated user life cycle management, and periodic user access reviews.

Section : 3.3.2 Application Access and Activity

Sub Sec.	Compliance requirements	How we can help?
1	Application shall prohibit users from logging into the application on more than one workstation at the same time with the same user-id.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options, including password-less and FIDO2-based authentication.

Cloud Security Policy

This policy maps the IAM capability that adheres to the IRDAI Information and Cyber Security Guidelines focusing on the strategic measures necessary for securing cloud-based environments within insurance companies.

Section : 3.4.1 Authentication

Sub Sec.	Compliance requirements	How we can help?
NA	It shall be ensured that the Cloud Service Provider supports various Multi-factor authentication mechanisms. Authorization shall be followed as per the existing "Information and Cyber Security Policy, Security Domain Policy, Section 2.2 subsection 3.2.2.3 Authrization Iventory." Organization shall affirm that the cloud service providers authentication process, access control, accountability and logging is in line with applicable regulatory and legal requirements. Customer data shall be protected from any unauthorized access.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options, including password-less and FIDO2-based authentication, for all on-prem, cloud-hosted, and SaaS applications and cloud Consoles.

Work From Remote Location

This policy maps the IAM capability that adheres to the IRDAI Information and Cyber Security Guidelines addressing the essential security measures required for employees working outside traditional office environments. This section highlights the importance of ensuring secure access to corporate resources, protecting sensitive data, and maintaining regulatory compliance while working remotely.

Section : 3.1 Framework

Sub Sec.	Compliance requirements	How we can help?
1	Board approved Cyber Security Policy (Policy) of the Insurer shall address risks associated with Work from Remote Location (WFRL) risks. The policy shall mandate the need to change passwords frequently.	The proposed IAM solution will address the policy requirement by implementing an appropriate strong password policy enforced by SSO.

Section : 3.2 Network Security

Sub Sec.	Compliance requirements	How we can help?
2	Authorized assets of the organization provided to the users shall be hardened as per security policy for strong password authentication.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options, including password-less and FIDO2-based authentication.

Section : 3.3 Data Management

Sub Sec.	Compliance requirements	How we can help?
1	Data containerization, Multifactor authentication and remote data wipe shall be done to prevent data tampering and misuse of lost mobile/tablet devices during the period when WFRL has been permitted by the entity.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options, including password-less and FIDO2-based authentication for mobile applications.

Section : 3.4 Human Resource Security

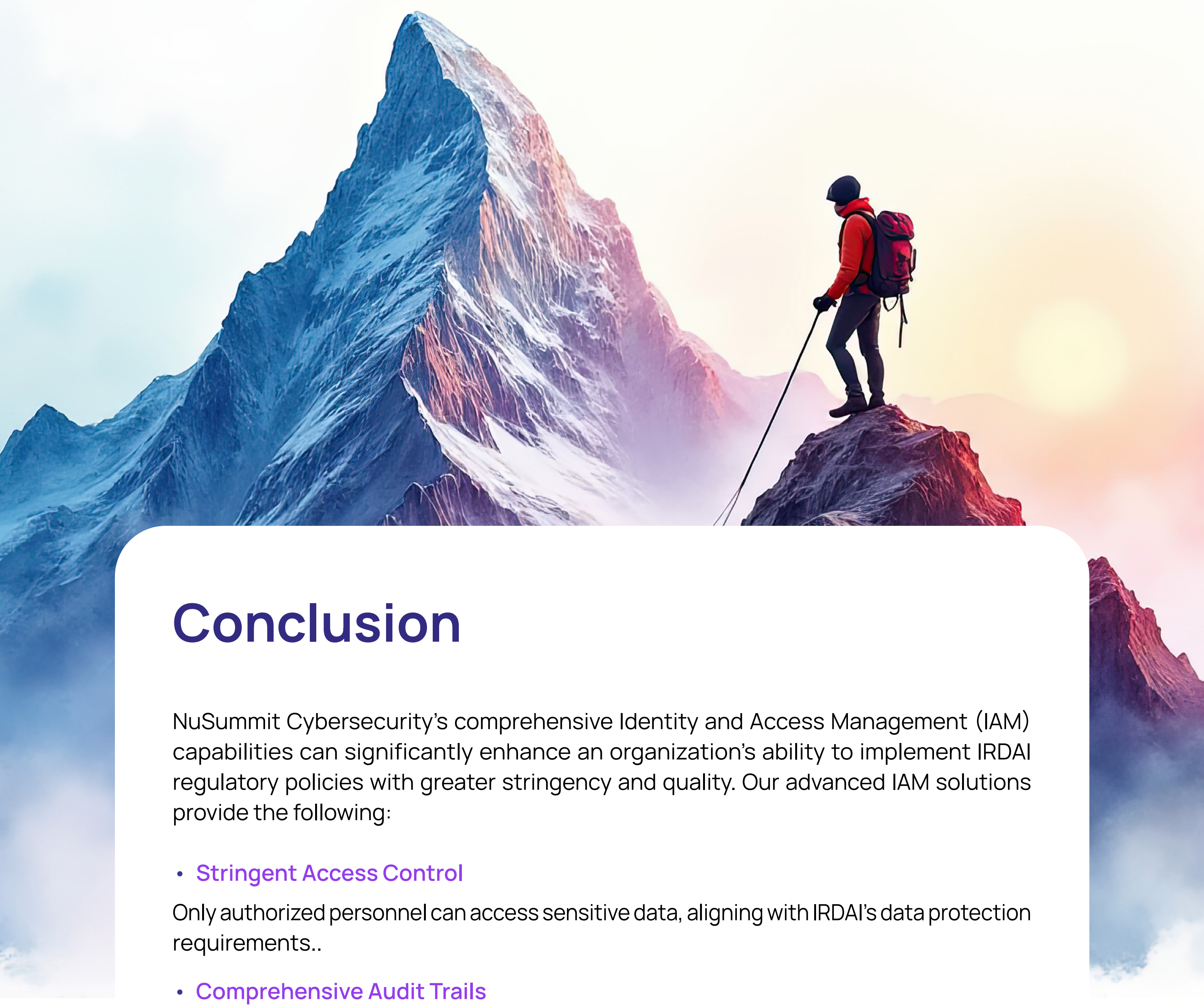
Sub Sec.	Compliance requirements	How we can help?
3	An audit of Privileged user-identity access authentication shall be conducted for administrative purposes.	The proposed IAM solution will address the policy requirement by implementing automated user life cycle management and periodic user access reviews for privileged users and accesses.

Dealing Room Operations

This policy maps the IAM capability that adheres to the IRDAI Information and Cyber Security Guidelines, which are designed to protect the integrity, confidentiality, and availability of dealing room systems and data while ensuring compliance with regulatory requirements, within insurance companies.

Section : 3.3 Data Security

Sub Sec.	Compliance requirements	How we can help?
3	Multi-factor authentication shall be enabled for all Bloomberg terminals.	The proposed IAM solution will address the policy requirement by implementing Single Sign-On and strong authentication using various MFA options including password-less and FIDO2-based authentication



Conclusion

NuSummit Cybersecurity's comprehensive Identity and Access Management (IAM) capabilities can significantly enhance an organization's ability to implement IRDAI regulatory policies with greater stringency and quality. Our advanced IAM solutions provide the following:

- Stringent Access Control

Only authorized personnel can access sensitive data, aligning with IRDAI's data protection requirements..

- Comprehensive Audit Trails

Enabling detailed tracking of user activities, supporting anti-money laundering efforts and fraud investigations.

- Automated Policy Enforcement

Implementing and maintaining IRDAI-compliant access policies across all systems.

- Multi-Factor Authentication

Strengthening security measures in line with IRDAI's cybersecurity guidelines.

- Identity Governance

Facilitating regular access reviews and role-based access control.

- Seamless Integration

Connecting diverse insurance systems to create a unified security framework, enhancing overall fraud prevention capabilities.

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at **cybersecurity.nusummit.com**
or write to us at **cybersales@nusummit.com**

Dallas I Jersey City I Cupertino I Ottawa I Riyadh I Dubai
Mumbai I New Delhi I Bangalore

Follow us at: