NetIQ® Identity Governance™ 3.5

Security Target

Date:	*July 13, 2020*
Version:	*2.7*
Prepared By:	*NetIQ Corporation*
Prepared For:	*NetIQ Corporation* *Suite 1200* *515 Post Oak Blvd* *Houston, Texas 77027*

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Identity Governance 3.5. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

Table of Contents **2**

1. Introduction **4**
1.1. ST Reference *4*
1.2. TOE Reference *4*
1.3. Document Organization *4*
1.4. Document Conventions *5*
1.5. Document Terminology *5*
1.6. TOE Overview *6*
1.7. TOE Description *7*
1.7.1. Overview 7
1.7.2. Console 11
1.7.3. Identity Governance engine (IG): 11
1.7.4. OSP engine (OSP): 11
1.7.5. Identity Reporting engine (IR): 11
1.8. Physical Boundary *11*
1.8.1. Hardware and Software Supplied by the IT Environment 12
1.8.2. Logical Boundary 13
1.8.3. TOE Security Functional Policies 14
1.8.4. TOE Product Documentation 14

2. Conformance Claims **15**
2.1. CC Conformance Claim *15*
2.2. PP Claim *15*
2.3. Package Claim *15*
2.4. Conformance Rationale *15*
2.5. Security Problem Definition *15*
2.6. Threats *15*
2.7. Organizational Security Policies *15*
2.8. Assumptions *16*

3. Security Objectives **17**
3.1. Security Objectives for the TOE *17*
3.2. Security Objectives for the Operational Environment *17*
3.3. Security Objectives Rationale *18*
3.3.1. Rationale for Security Threats to the TOE 18

4. Extended Components Definition **21**

5. Security Requirements **22**
5.1. Security Functional Requirements *22*
5.1.1. Security Audit (FAU) 22
5.1.2. Identification and Authentication (FIA) 22
5.1.3. Security Management (FMT) 23
5.2. Security Assurance Requirements *23*
5.3. Security Requirements Rationale *24*
5.3.1. Security Functional Requirements 24
5.3.2. Dependency Rationale 24
5.3.3. Sufficiency of Security Requirements 25
5.3.4. Security Assurance Requirements Rationale 26

5.3.5. Security Assurance Requirements Evidence 26

6. TOE Summary Specification 28

6.1. TOE Security Functions 28

6.2. Security Audit 28

6.3. Identification and Authentication 29

6.4. Security Management 29

7. Appendix A: Privileges (Authorizations) 30

8. Appendix B: Role Descriptions 32

9. Appendix C: Privilege to Role Mapping 34

List of Tables

Table 1 – ST Organization and Section Descriptions 5
Table 2 – Acronyms Used in Security Target 6
Table 3 – Evaluated Configurations for the TOE 12
Table 4 – IT Environment 13
Table 5 – Logical Boundary Descriptions 14
Table 6 – Threats Addressed by the TOE 15
Table 7 – Organizational Security Policies 15
Table 8 – Assumptions 16
Table 9 – TOE Security Objectives 17
Table 10 – Operational Environment Security Objectives 17
Table 11 – Mapping of Assumptions, Threats, and OSPs to Security Objectives 18
Table 12 – Mapping of Threats, Policies, and Assumptions to Objectives 20
Table 13 – TOE Security Functional Requirements 22
Table 14 – Security Assurance Requirements at EAL2 24
Table 15 – Mapping of TOE Security Functional Requirements and Objectives 24
Table 16 – Rationale for TOE SFRs to Objectives 26
Table 17 – Security Assurance Rationale and Measures 27
Table 18 – Security Management Functions and SFRs 29

List of Figures

Figure 1 – Basic Identity Governance 3.5 Configuration 8

Figure 2 – Functional Block Diagram 9

Figure 3 – IG Sample Data Flow 10

Figure 4 – TOE Boundary 12

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1. ST Reference

ST Title	NetIQ® Identity Governance 3.5
ST Revision	2.7
ST Publication Date	July 13, 2020
Author	Michael F. Angelo

1.2. TOE Reference

TOE Reference	NetIQ® Identity Governance 3.5
TOE Developer:	NetIQ Corporation
Evaluation Assurance Level (EAL):	EAL 2+

Note: The official name of the product is: NetIQ Identity Governance 3.5 (aka Identity Governance 3.5). The released product server component can be uniquely identified as: NetIQ Identity Governance 3.5.1_33625 and the client component can be identified as NetIQ Identity Governance 3.5.1_33627. The product name may also be referred to as Identity Governance 3.5 and abbreviated as simply Identity Governance or IG. The Identity Governance 3.5 client help about identifies the product as:

- Identity Governance client version 3.5.1 was built Sat April 6 2019 9:46 AM from revision 33625

The Identity Governance 3.5 server help about identifies the product as:

- Identity Governance server version 3.5.1 was built on Sat April 6 2019 7:58 PM from revision 33627

For the purpose of this document all of the above references are equivalent, and the document may refer to the product simply as Identity Governance or the TOE.
Note: The file download name is: identity-governance-3.5-win.zip.
Note: The above listed identities include components (Identity Reporting (IR), Identity Governance Server (IG), and One Signon Service Provider (OSSP).

1.3. Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats

SECTION	TITLE	DESCRIPTION
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4. Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text in square brackets.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5. Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
AD	Active Directory
AMQP	ActiveMQ Protocol also known as Active Message Queuing Protocol (on top of HTTPS / TLS) and is used for reliable email.
CC	Common Criteria version 3.1
DaaS	Directory as a Service
DTP	Data Transformation and Processing Service
EAL	Evaluation Assurance Level
eDir	eDirectory

TERM	DEFINITION
IR	Identity Reporting
IG	Identity Governance
NTP	Network Time Protocol
OSP	One SSO Provider
OSSP	One Signon Service Provider
SFP	Security Function Policy
SFR	Security Functional Requirement
SSO	Single Sign On
SoD	Separation of Duties
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
URI	Universal Resource Indicator

Table 2 – Acronyms Used in Security Target

1.6. TOE Overview

NetIQ® Identity Governance™ 3.5 provides centralized identity and authorization administration as well as governance functions, in short the interface for identity governance management tasks. These tasks span most business processes for identity, access, and access certification. The TOE enables the user to demonstrate compliance for access certification and re-certification projects. The TOE, already identified in section 1.2 as NetIQ Identity Governance 3.5.1_33625 (including components[1] Identity Governance Server (IG), Identity Reporting (IR), and One Signon Service Provider (OSSP)) and the client component as NetIQ Identity Governance 3.5.1_33627. The TOE provides the following management functions:

- audit
- automatic notification (for task tracking), with visual timelines and a mechanism for issue escalation
- automatic access certification processes and reports
- collection, management, and correlation of user entitlements across on-premises and cloud applications
- reporting (contextual / analytics / forensics)
- business policy management (including roles, SoD, risk scoring)
- management of access requests (and associated policies / handling)

The TOE also provides functionality for high-risk entitlements - such as Separation of Duties (SoD) violations or processing of orphan accounts.
Finally, the TOE reduces issues with excessive access by using automated revocation features.

The TOE (IG) provides identity and authorization administration as well as governance functions. It provides the ability to define roles, implement separation of duties, manage access controls [2] over a large number of resources, and audit user access. This in turn, assists in demonstrating adherence to compliance requirements.

[1] These components do not require manual patching and are updated as part of installation and or update.
[2] For the general user population, the TOE modifies the environment to enable or disable general user access controls. The environment enforces the access controls that IG Manages.

In summary, the TOE (Identity Governance) collects information from various application data sources and manages the entire access governance, risk, and compliance process. Identity Governance provides tools to guide you through the key phases of the access review and validation process. Identity Governance integrates with NetIQ Identity Manager so you can grant and revoke access in real time and mitigate risk.

The TOE requires the following systems in the operating environment: a Database, Authentication server, and Audit server.

The following is a usage scenario that provides insight into how the system is run.
The players:

- IG admin used to install and configure the initial package
- global admin used for issuing privileges (which is synonymous with Authorizations) and day to day maintenance.
- Reviewer – reviews and denies or rejects requests
- Review Owner – provides oversight on requests and either approves the Reviewer's decision or overrides it. The Review Owner is responsible for reviewing the results from the Verifier.
- Auditor – looks at the request and flow noting anomalies
- The Fullfiller – implements the change and logs status
- Verifier – automatic system process – identifying that the item activity is complete. And posts a status for the Review Owner.

Example workflow:

The first mode is an Access Request. This enables users to request permissions. When in actual use a user accessing a remote application will not see anything different if they are given access. If they are not given access, they will see a normal rejection message as provided by the remote application. When the request is made, it can go through an approval process starting with the Reviewer. The Reviewer will approve or reject the request. The Review Owner will approve or reject the Reviewers decision. The Fulfiller will implement the change and log its status. The Auditor will make sure the process flow was correct and that no anomalies occurred, and that no rules are being violated. The Verifier ensures that the activity completed and provides a status for the Review Owner.

The second mode of use is to review all of the user access to a permission. This allows the Review Owner to see all of the users with specific permission, and adjust accordingly.

1.7. TOE Description

1.7.1. Overview

The TOE consists of the following components:

- NetIQ Identity Governance server component:
  - Identity Governance
  - OSP
  - Identity Reporting
- NetIQ Identity Governance client component:
  - Console (web UI – Governance and Administrator)

The TOE also requires a Database, Authentication, and Audit server which are not part of the TOE.

The basic configuration is depicted in the figure[3] below:

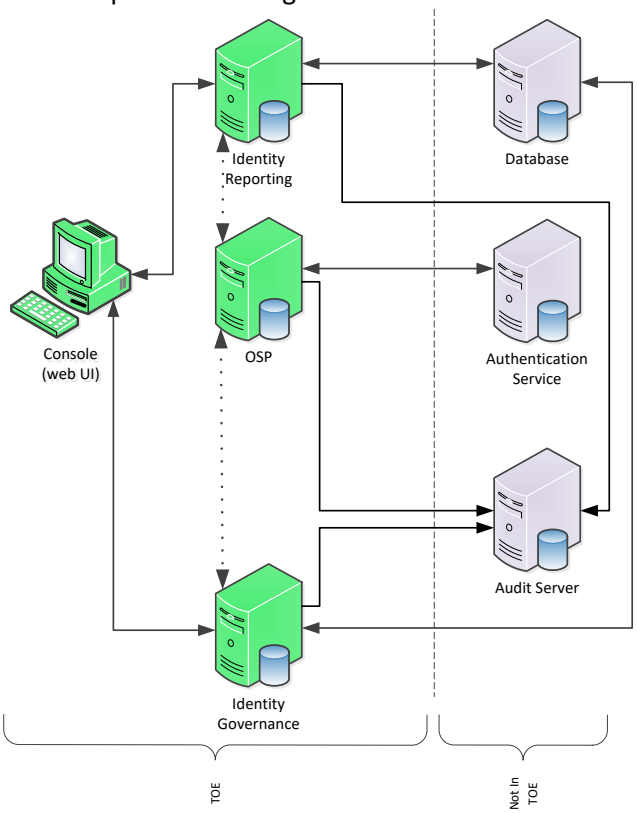

Figure 1 – Basic Identity Governance 3.5 Configuration

It is important to note that all components in the Identity Governance architecture can scale with multiple instances of the components.

The following diagram reflects the functional blocks in the configuration:

[3] Components that are not part of the TOE are to the right of the dotted line and are Grey. These components are included in this diagram for completeness of documentation.

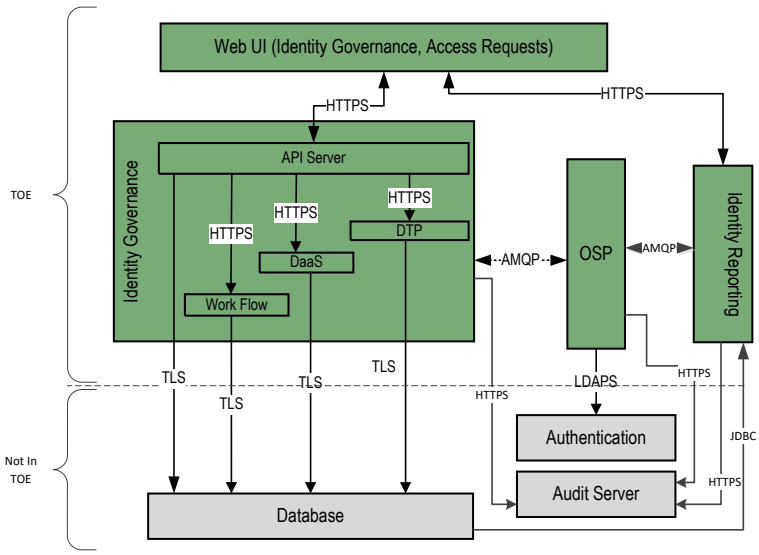

Figure 2 – Functional Block Diagram[4]

It is important to note that, while the TOE uses TLS / HTTPS for communications with systems in the operating environment, their cryptographic services are outside the scope of the evaluation.

Identity Governance works by:

1. Obtaining authentication tokens from an authentication service.
2. Reviewing the authentication token and obtaining the associated authorization (synonymous with privileges) information.
3. Presenting the associated authorizations to the user.

The Identity Governance architecture enables the user to provide the following features:

1. audit
2. automatic notification (for task tracking), with visual timelines and a mechanism for issue escalation
3. automatic access certification processes and reports
4. collection, management, and correlation of user entitlements across on premise and cloud applications
5. reporting (contextual)
6. risk scoring
7. user roles

[4] All communications from the console are via HTTPS

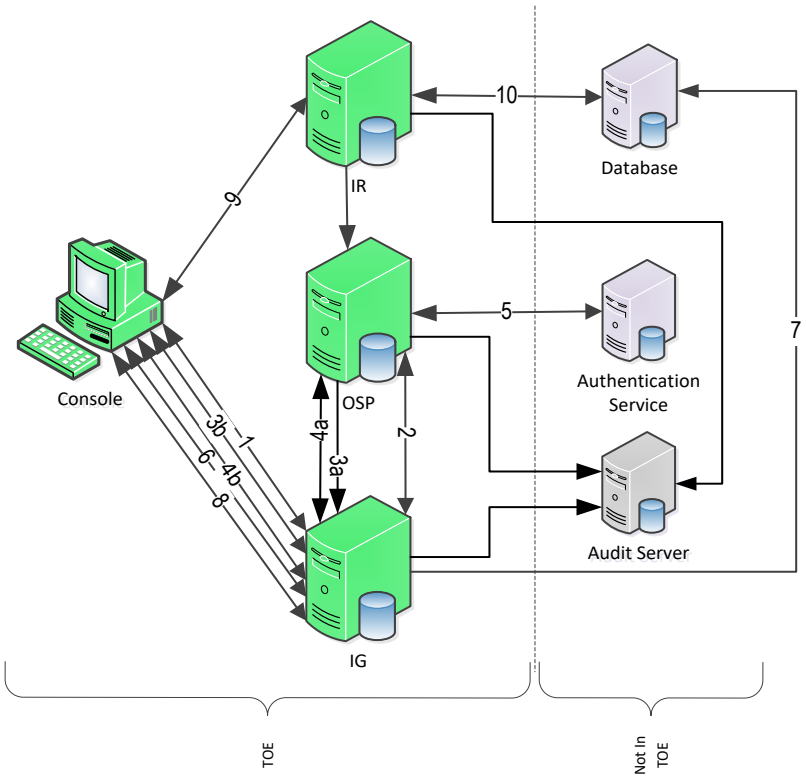

Figure 3 – IG Sample Data Flow

The following describes the data flow

1. The user connects Console and sends an OAuth token, if available (1).
2. Identity Governance engine (1) validates the OAuth token
    - On Success
        - It forwards it to OSP (2)
    - On Failure:
        - The OSP forwards a login screen in an iFrame to the console via IG (4a/4b)
        - User provides credentials to OSP (4b - IG acts as a pass-through)
        - The OSP forwards the credentials to the Authentication Service (5).
        - The OSP provides the authentication token (bearer token) to the console via the IG (4a,4b)
        - The console includes the bearer token for all requests to the Identity Governance engine (IG) (6)
        - The IG engine confirms / displays the user roles in the database (3a/3b)
        - On Failure:
            - If a user fails their logon attempt, the TOE presents a message saying 'Failed Login, please try again".
3. The Console can perform the relevant tasks and roles as allowed.
        - Examples include initiator, reviewer, specifying approvers, approving.
4. Transactions flow through the IG to the database via lines 7 and 8.

5. Requests for Reporting services go from the console directly to the IR engine. Shown in line 9. The IR generates reports from information in the database via line 10[5].

1.7.2. Console

The Console enables authorized users to access the IG system, the OSP, and the IR.

1.7.2.1. Administrator

IG Admin and Global Administrators (aka Business Administrators) can perform any of the functions on the system.

Business Administrators are described in Appendix A: Privileges (Authorizations) with the privilege and subject relationships being described in Appendix C: Privilege to Role Mapping.

1.7.2.2. User

User roles are described in Appendix B: Role Descriptions.

1.7.3. Identity Governance engine (IG):

Identity Governance is an administrative tool responsible for:

- forwarding the URI to the console
- obtaining the associated roles from the database
- evaluating the roles based on the user identity
- returning the roles to the user as appropriate
- enforcing the roles
- performing the actions associated with the roles

1.7.4. OSP engine (OSP):

The OSP is responsible for:

- proxy of authentication requests between the Console and the Authentication Service
- generating a Bearer Token

1.7.5. Identity Reporting engine (IR):

The Identity reporting engine is responsible for:

- Generating reports of roles and provides information about transactions.

1.8. Physical Boundary

The TOE is a software TOE and includes the following components:

- Console
- Identity Governance engine (IG)
- One SSO Provider engine (OSP)
- Identity Reporting engine (IR)

The following figure presents the TOE diagram.

[5] Requires roles. (global or report admin)

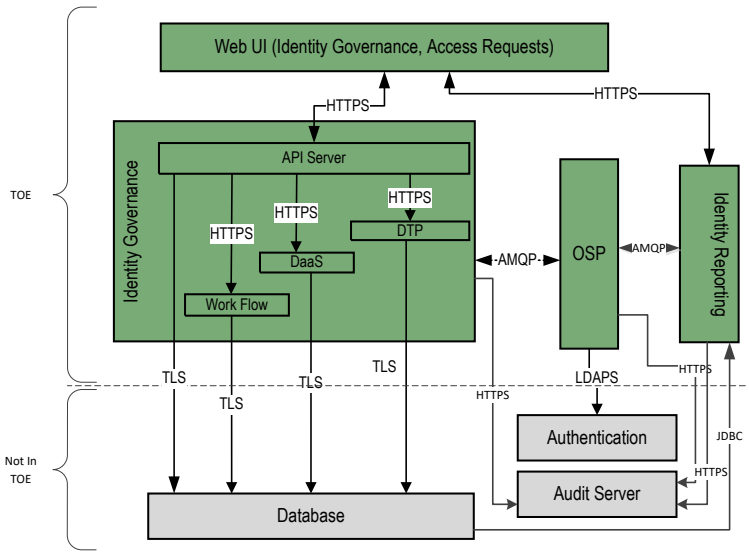

Figure 4 – TOE Boundary

The evaluated configuration of the product will consist of the product as depicted in Figure 1.

COMPONENT	VERSION NUMBER
Identity Governance	Version 3.5.1
Identity Reporting	Version 6.5.0
OSP	Version 6.2.0
Console	Version 3.5.1

Table 3 – Evaluated Configurations for the TOE

Note the following constraints for the evaluated configuration:

The hardware, operating systems and third-party support software on each of the systems are excluded from the TOE boundary.

The IG package is delivered via the web as a zip file. This file must be expanded and the various elements installed. The documentation is available on the web. For addition information please see the product guidance documents.

1.8.1. Hardware and Software Supplied by the IT Environment

The TOE consists of a set of software applications. The hardware, operating systems and all third-party support software (e.g., Database, Identity Service (i.e. AD) and audit server) on the systems on which the TOE executes are excluded from the TOE boundary.

The TOE requires the following minimum hardware and software configuration:

TOE COMPONENT	TYPE	VERSION/MODEL NUMBER
Identity Governance	Operating System	Windows Server 2016 SLES 15 RHEL 7 Tomcat 9.0.12 ActiveMQ 5.12.1
	CPU	8.0 GHz, single processor
	Memory	32GB
	Storage	50GB
OSP	Operating System	Windows Server 2016
	CPU	8.0 GHz, single processor
	Memory	32GB
	Storage	100GB
Identity Reporting	Operating System	Windows Server 2016
	CPU	Pentium 4
	Memory	16 GB
	Storage	50 GB
Console	Operating System	Windows 10

Table 4 – IT Environment

1.8.2. Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following table:

TSF	DESCRIPTION
Security Management	The TOE provides Identity Governance administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to management of events and activities. Administrators configure the TOE with the Console via Web-based connection. The TOE enables Identity Governance administrators to define roles and associate entitlements (as in access within the process/program as opposed to roles outside of the program). The TOE also allows Identity Governance administrators to modify Identity Governance users and associate privileges (i.e. roles). The TOE provides 'check and balance' processes with strict separation of duties for activities that Identity Governance users perform. For example, one IG Operator would modify a user, while another IG Operator would review the modification and mark it as being ready for approval, while another IG Operator would need to approve it, while another IG Operator would audit the entire transaction.
Security Audit	The TOE provides audit data to track the activities of IG user roles. The TOE supports the provision of log data from each system component, such as an IG user accessing the IG system, IG user transactions (event/ticket management), as well as IG Administrators modifying IG users. The TOE also records security events such as IG access failed login attempts and transactions (via OSP). Audit data is stored for later review and analysis.

TSF	DESCRIPTION
Identification, Authentication, Authorization	The TOE enforces individual I&A functionality in conjunction with individuals or a group of users (called authorization assignments). Users must successfully authenticate using a unique identifier and password prior to performing any actions on the TOE.

Table 5 – Logical Boundary Descriptions

1.8.3. TOE Security Functional Policies

The TOE does not support any Security Functional Policies.:

1.8.4. TOE Product Documentation

The TOE includes the following product documentation[6]:

- NetIQ Identity Governance 3.5.1 Release Notes April 2019
- NetIQ Identity Governance Installation Guide, February 2020
- NetIQ® Identity Governance User Guide, June 2019
- NetIQ® Identity Governance Administrator Guide, June 2019
- NetIQ Identity Governance Identity Reporting Guide March 2018
- NetIQ® Identity Manager Driver for Identity Governance Implementation Guide December 2018
- NetIQ® Identity Governance™ 3.5 Operational User Guidance and Preparative Procedures Supplement (AGD_OPE / AGD_PRE) (Version 1.2)

[6] https://www.netiq.com/documentation/identity-governance-35/

2. Conformance Claims

2.1. CC Conformance Claim

The TOE is conformant to Common Criteria Version 3.1 Revision 5 (April 2017) Part 2 and Part 3 conformant.

2.2. PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3. Package Claim

The TOE claims conformance to the EAL2 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 5 (April 2017). The TOE does not claim conformance to any functional package. The TOE EAL2 assurance package is augmented with ALC_FLR.1.

2.4. Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

2.5. Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

2.6. Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.NO_AUTH	An unauthorized user may gain access to the TOE and alter the TOE configuration.
T.NO_PRIV	An authorized user of the TOE exceeds his/her assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data.

Table 6 – Threats Addressed by the TOE

2.7. Organizational Security Policies

The TOE meets the following organizational security policies:

ASSUMPTION	DESCRIPTION
P.EVENTS	All transactions from the TOE shall be captured, monitored and reported.
P.ACTIVITIES	All transactions (collection, management, and correlation of user entitlements) will be correlated and classified as activities and should be managed to resolution.

Table 7 – Organizational Security Policies

2.8. Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.MANAGE	Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner. Administrators of the TOE may only execute management workflow activities.
A.NOEVIL	Administrators of the TOE and operators on the local area network are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation. Administrators and TOE Users will not leave their systems unattended and unlocked.
A.LOCATE	The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access.
A.CONFIG	The TOE environment is properly configured to provide access to the TOE.
A.TIMESOURCE	The TOE environment has a trusted source for system time via NTP server
A.UPDATE	The TOE environment is regularly updated by an administrator to address potential and actual vulnerabilities.

Table 8 – Assumptions

3. Security Objectives

3.1. Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.AUDIT	The TOE shall collect data from all TOE activities including changes to permissions or privileges and provisioning of access.
O.MANAGE_ ACTIVITIES	The TOE shall provide workflows to manage TOE activities including all transactions such as the collection, management, and correlation of user entitlements.
O.SEC_ACCESS	The TOE shall ensure that only those authorized users and applications are granted access to security functions and associated data.

Table 9 – TOE Security Objectives

3.2. Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.TIME	The TOE operating environment shall provide an accurate timestamp (via reliable NTP server).
OE.CONFIG	The TOE environment is properly configured to be able to access the TOE.
OE.ENV_PROTECT	The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.
OE.PERSONNEL	Authorized administrators are trained, non-hostile and follow all administrator guidance and must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted to not disclose their authentication credentials to any individual not authorized for access to the TOE. Authorized administrators are also required to manage and administer the TOE in a secure manner. Authorized administrators must be competent and security aware personnel in accordance with the administrator documentation
OE.PHYSEC	The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility
OE.UPDATE	The TOE operational environment is updated by an administrator to address potential and actual vulnerabilities.

Table 10 – Operational Environment Security Objectives

3.3. Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

OBJECTIVES / ASSUMPTIONS/ THREATS/ POLICIES	O.AUDIT	O.MANAGE_ACTIVITIES	O.SEC_ACCESS	OE.TIME	OE.CONFIG	OE.ENV_PROTECT	OE.PERSONNEL	OE.PHYSEC	OE.UPDATE
A.CONFIG					✓				
A.MANAGE							✓		
A.NOEVIL							✓		
A.LOCATE								✓	
A.TIMESOURCE				✓					
A.UPDATE									✓
T.NO_AUTH	✓		✓			✓	✓	✓	
T.NO_PRIV	✓		✓						
P.EVENTS	✓			✓			✓		
P. ACTIVITIES		✓		✓			✓		

Table 11 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

3.3.1. Rationale for Security Threats to the TOE

ASSUMPTION/ THREAT/ POLICY	RATIONALE
A.CONFIG	This assumption is addressed by • OE.CONFIG which ensures that the TOE environment (including but not limited to the AD/LDAP and DB servers) is configured appropriately to access the TOE.
A.MANAGE	This assumption is addressed by • OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.NOEVIL	This assumption is addressed by • OE.PERSONNEL, OE.PERSONNEL needs to address the need for administrators to not be careless, willfully negligent or hostile
A.LOCATE	This assumption is addressed by • OE.PHYSEC which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
A.TIMESOURCE	This assumption is addressed by • OE.TIME, which ensures the provision of an accurate time source.

ASSUMPTION/ THREAT/ POLICY	RATIONALE
A.UPDATE	This assumption is addressed by OE. UPDATE. • OE.UPDATE which requires the TOE operational environment be updated regularly to address potential and actual operational security issues.
T.NO_AUTH	This threat is countered by the following: • O.AUDIT, which ensures that all TOE transactions and attempted transactions are auditable and • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications and • OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed and • OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner and • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
T.NO_PRIV	This threat is countered by • O.AUDIT which ensures that all TOE transactions and attempted transactions are auditable and • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.
P.EVENTS	This organizational security policy is enforced by • O.AUDIT, which ensures that the TOE collects activities from all TOE operations and • OE.TIME, which provides support for enforcement of this policy by ensuring the provision of an accurate time source and • OE.PERSONNEL, which ensures that authorized administrators are non-hostile and follow all administrator guidance and ensures that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

ASSUMPTION/ THREAT/ POLICY	RATIONALE
P. ACTIVITIES	This organizational security policy is enforced by • O.MANAGE_ACTIVITIES, which ensures that the TOE will provide the capability to manage all activities including all transactions such as the collection, management, and correlation of user entitlements and • OE.TIME, which ensures that the TOE operating environment shall provide an accurate timestamp (via reliable NTP server) for auditing and • OE.PERSONNEL, which ensures that authorized administrators are non-hostile and follow all administrator guidance and ensures that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

Table 12 – Mapping of Threats, Policies, and Assumptions to Objectives

4. Extended Components Definition

There are no extended components defined.

5. Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

5.1. Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.2	User Authentication before Any Action
	FIA_UID.2	User Identification before Any Action
Security Management	FMT_MOF.1	Management of Security functions behavior
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 13 – TOE Security Functional Requirements

5.1.1. Security Audit (FAU)

5.1.1.1. FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit features[7];
b) All auditable events for the [*not specified*] level of audit; and
c) [events as required by FMT]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other audit relevant information].

5.1.1.2. FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [the Administrator and privileged users with Privileges as described in Appendix A: Privileges (Authorizations)] with the capability to read [transactional audit data] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.2. Identification and Authentication (FIA)

5.1.2.1. FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User Name, Privileges, Role].

[7] There is no capability to start up or shut down the audit, except as part of the normal execution of the product.

5.1.2.2. FIA_UAU.2 User Authentication before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.2.3. FIA_UID.2 User Identification before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.3. Security Management (FMT)

5.1.3.1. FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behavior of, disable, enable, modify the behavior of*] the functions [as defined in Appendix B: Role Descriptions] to [Assigned Roles as described in Appendix C: Privilege to Role Mapping].

5.1.3.2. FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [*query* ,[*add, remove, manage*]] the [authorizations as described in Appendix A: Privileges (Authorizations)] to [Roles as described in Appendix C: Privilege to Role Mapping].

5.1.3.3. FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the management functions: [As described in Appendix B: Role Descriptions].

5.1.3.4. FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [described in Appendix A: Privileges (Authorizations) and Appendix B: Role Descriptions as controlled by Appendix C: Privilege to Role Mapping].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2. Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.1	Flaw Remediation Procedures

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 14 – Security Assurance Requirements at EAL2

5.3. Security Requirements Rationale

5.3.1. Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE / SFR	O.AUDIT	O.MANAGE_ACTIVITIES	O.SEC_ACCESS
FAU_GEN.1	✓		
FAU_SAR.1	✓		✓
FIA_ATD.1			✓
FIA_UAU.2			✓
FIA_UID.2			✓
FMT_MOF.1		✓	✓
FMT_MTD.1		✓	✓
FMT_SMF.1		✓	
FMT_SMR.1			✓

Table 15 – Mapping of TOE Security Functional Requirements and Objectives

5.3.2. Dependency Rationale

This ST satisfies all the security functional requirement dependencies of the Common Criteria. The table below lists each SFR to which THE TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FAU_GEN.1	FPT_STM.1	YES	Satisfied by the Operational Environment (OE.TIME)
FAU_SAR.1	FAU_GEN.1	YES	
FIA_ATD.1	N/A	N/A	

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FIA_UAU.2	FIA_UID.1	YES	Satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1
FIA_UID.2	N/A	N/A	
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	YES	
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	YES	
FMT_SMF.1	N/A	N/A	
FMT_SMR.1	FIA_UID.1	YES	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.

5.3.3. Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

Objective	RATIONALE
O.AUDIT	The TOE shall collect data from activity in IG. This includes tracking changes to the system, and information, updating titles, etc. Following security requirements • FAU_GEN.1 and FAU_SAR define the auditing capability for events, administrative and user access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs
O.MANAGE_ACTIVITIES	The objective to ensure that the TOE can manage all activities and is met by the following security requirements: • FMT_MTD.1 restricts the ability to *query, add, remove, manage* TSF data to users authorized as described in Appendix A: Privileges (Authorizations) to roles as described in Appendix C: Privilege to Role Mapping. • FMT_MOF.1 restricts the ability to query, add, remove, and manage the functions in Appendix B: Role Descriptions to users assigned role as defined in Appendix C: Privilege to Role Mapping. • FMT_SMF.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role.

Objective	RATIONALE
O.SEC_ACCESS	This objective ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications. • FIA_UAU.2 requires the TOE to enforce authentication of all users prior to configuration of the TOE • FIA_UID.2 requires the TOE to enforce identification of all users prior to configuration of the TOE • FIA_ATD.1 specifies security attributes for users of the TOE • FMT_MTD.1 restricts the ability to query, add, remove, manage TSF data to users authorized as described in Appendix A: Privileges (Authorizations) to roles as described in Appendix C: Privilege to Role Mapping. • FMT_MOF.1 restricts the ability to access the functions in Appendix B: Role Descriptions to users' assigned roles as defined in Appendix C: Privilege to Role Mapping. • FMT_SMR.1 supports the security functions relevant to the TOE and ensure the definition of an authorized administrator role.

Table 16 – Rationale for TOE SFRs to Objectives

5.3.4. Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 2. EAL2 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering a reduced exposure for an attacker to subvert the security policies without physical access.

5.3.5. Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
Security Architecture Description (ADV_ARC.1)	NetIQ® Identity Governance™ 3.5 *Security Architecture* (ADV_ARC) Version 1.0
Security Enforcing Functional Specification (ADV_FSP.2)	NetIQ® Identity Governance™ 3.5 *Functional Specification* (ADV_FSP) Version 1.0 NetIQ® Identity Governance™ 3.5 FSP Appendix A Version 1.0

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
Architectural Design (ADV_TDS.1)	NetIQ® Identity Governance™ 3.5 *Architectural Design* (ADV_TDS) Version 1.0
Operational User Guidance (AGD_OPE.1)	NetIQ® Identity Governance™ 3.5 *Operational User Guidance and Preparative Procedures Supplement (AGD_OPE)* Version 1.0 NetIQ® Identity Governance User Guide February 2018 Installation and Configuration Guide NetIQ® Identity Manager Driver for NetIQ Access Review March 2016
Preparative Procedures (AGD_PRE.1)	NetIQ® Identity Governance™ 3.5 *Operational User Guidance and Preparative Procedures Supplement (AGD_OPE)* Version 1.0 NetIQ® Identity Governance User Guide February 2018 Installation and Configuration Guide NetIQ® Identity Manager Driver for NetIQ Access Review March 2016
Use of a CM system (ALC_CMC.2)	NetIQ® Identity Governance™ 3.5 Document Configuration Management Processes and Procedures (ALC_CM) Version 2.0
Parts of the TOE CM coverage (ALC_CMS.2)	NetIQ® Identity Governance™ 3.5 Document Configuration Management Processes and Procedures (ALC_CM) Version 2.0
Delivery Procedures (ALC_DEL.1)	NetIQ® Identity Governance™ 3.5 *Delivery Processes and Procedures* (ALC_DEL) Version 1.0.
Flaw Remediation Procedures (ALC_FLR.1)	NetIQ® Identity Governance™ 3.5 *Basic Flaw Remediation Procedures (ALC_FLR)* Version 1.0.
ATE_COV.1 Evidence of Coverage	NetIQ® Identity Governance™ 3.5 *Test Plan and Coverage Analysis (ATE)* Version 0.5.
ATE_FUN.1 Functional Testing	NetIQ® Identity Governance™ 3.5 *Test Plan and Coverage Analysis (ATE)* Version 0.5

Table 17 – Security Assurance Rationale and Measures

6. TOE Summary Specification

This section presents the Security Functions implemented by the TOE. For the purpose of this TOE the CONSOLE is a GUI that is executed in a web browser.

6.1. TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Identification and Authentication
- Security Management

6.2. Security Audit

The TOE provides audit data to track the activities of IG user roles. The TOE supports the provision of log data from each system component, such as an IG user accessing the IG system, IG user transactions (event/ticket management), as well as IG Administrators modifying IG users. The TOE also records security events such as IG access failed login attempts and transactions (via OSP).

Audit data is stored for later review and analysis.

- Audit Events are generated internally. Each time an audited method is called or an audited data object is modified, IG generates audit events. There are two types of Audit Events. One which monitors user actions for example, user login/out, add/delete user and another which monitors system actions/health, for example, process start/stop. Audit Events are logged into log files, saved into a database.

Audit Events record the date and time of the event, type of event, subject identity and outcome.

The TOE generates the following audit data:

- Start-up and shutdown of the audit functions[8].
- All auditable events for the [*not specified*] level of audit; and
- events generated by management functions as described in FMT_MOF.1, FMT_MTD.1, and FMT_SMF.1 and stated in FAU_GEN.1.

The TOE provides a user with privileges as defined in Appendix A: Privileges (Authorizations) the capability to read all audit data generated within the TOE via the Console. The GUI provides a suitable means to interpret the information from the audit log.

The TOE provides users with the capability for basic audit review. Advanced review requires the use of a SIEM to filter audit event data queries and provide advanced searches.

The TOE ensures that the audit trail data is date / time stamped when recorded with a dependable date and time received from the OE (operating system). In this manner, accurate time and date is maintained on the TOE.

The ability to review application and administrative audit data is limited to the IG admin and IG Administrator. Management audit review (i.e. Login / logout into IG, etc..) is provided by the environment while the TOE provides the ability to review transactional audit data (i.e. granting of access, etc..).

The Security Audit function is designed to satisfy the following security functional requirements:

[8] In order for the configuration change to be activated, a re-start of the TOE is required.

- FAU_GEN.1
- FAU_SAR.1

6.3. Identification and Authentication

The TOE enforces individual identification and authentication and provides a centralized authentication mechanism. Once identification and authentication are verified by Authentication Service[9], the TOE provides a token with the user's authorizations. Users with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE. The TOE maintains authorization information that determines which TOE functions an authenticated administrator or user (of a given role) may perform. If a user is not explicitly in the TOE with a privilege as described in Appendix A, they have no abilities with-in the TOE, but can still be acted on or managed by the TOE.

The TOE maintains the following list of security attributes belonging to individual users:

- User Identity (i.e., user name)
- Privileges
- Role

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2

6.4. Security Management

The Console provides a user interface that administrators may use to manage TOE functions. The Console provides web-based access to TOE functions through supported web browsers. The TOE provides management functions for the IR, IG, OSP via the console. The console cannot manage the OSP, but it can be configured to use it. The OSP is dynamically fed by mining the back-end identity database. The associated SFRs are noted in the table below.

Functional Description	SFR
The TOE provides administrators and users with privileges as described in Appendix A: Privileges (Authorizations)] with the capability to read audit data in a manner suitable to be interpreted.	FAU_SAR.1
The TOE restricts the ability to control the functions as described in Appendix B: Role Descriptions according to roles as described in Appendix C: Privilege to Role Mapping.	FMT_MOF.1
Only the Administrator and privileged users with Authorizations as described in Appendix A: Privileges (Authorizations) can control user privileges and user accounts attributes.	FMT_MTD.1
The TOE supports the following management functions as described in Appendix A: Privileges (Authorizations) and Appendix B: Role Descriptions.	FMT_SMF.1
The TOE provides roles as described in Appendix A: Privileges (Authorizations) and Appendix B: Role Descriptions with relationships as described in Appendix C: Privilege to Role Mapping.	FMT_SMR.1

Table 18 – Security Management Functions and SFRs

[9] The Authentication services depend on a back-end service such as Active Directory.

7. Appendix A: Privileges (Authorizations)

Global Administrator

The Global Administrator (in the documentation may be referred to as a Business Administrator) is the primary authorization and can:

- Perform all Identity Governance actions
- Assign all Identity Governance global and runtime authorizations

Access Request Administrator

The Access Request Administrator manages defining who can request access in your enterprise. This authorization can:

- Create, modify, and delete Access Request Policies
- Create, modify, and delete Access Request Approval Policies
- Edit the default Access Request Approval Policy

Auditor

The Auditor has read-only rights to the catalog, reviews, separation of duties policies and violations, fulfillment status, and the Overview. However, an account assigned to the Auditor authorization might also be specified as a Review Auditor in a review definition.

Business Roles Administrator

The Business Roles Administrator performs all administrative functions for all business roles. A Business Roles Administrator can delegate administrative privileges. This authorization can:

- Create a business role
- Modify a business role
- Add or change role owners, fulfillers, and categories
- Add or change the business role approval policy
- Add users and groups to the business role
- Exclude users and groups from the business role
- Publish a business role
- Delete a business role
- Configure the business roles default approval policy
- Create and modify business roles approval policies

Data Administrator

The Data Administrator manages the identity and application data sources. This authorization can:

- Create, add, modify, and review data sources
- Create scheduled collections
- Execute data collection and publishing
- Create and map attributes in the catalog
- Review and edit data in the catalog
- Delegate responsibility by assigning application administrators, application owners, or manual fulfillers to applications in the catalog
- View data collection, data summary, and system trends in the Overview

Fulfillment Administrator

The Fulfillment Administrator manages fulfillment and verification of requests that result from reviews. This authorization can:

- Access real time and historical data for provisioning activities, including fulfillment status and verification management

Report Administrator

The Report Administrator can access Identity Reporting. This authorization can:

- Create, view, and run reports for Identity Governance

Review Administrator

The Review Administrator manages the review process but does not have access to data collection or fulfillment settings. This authorization can:

- Create, schedule, and start reviews
- Modify a review schedule
- Assign all the runtime authorizations as part of a review, thereby delegating certain rights pertaining to the review to those authorizations
- View running reviews
- View data summary and system trends in the Overview
- View the Catalog but cannot modify it

Technical Roles Administrator

The Technical Roles Administrator creates and manages technical roles.

Security Officer

The Security Officer has read-only rights to the catalog and can:

- Modify all configuration settings
- Assign authorizations for all functions in Identity Governance
- Add or remove account categories
- View data summary in the Overview
- View the Catalog but cannot modify it

NOTE: Ensure that the users assigned to the Security Officer authorization can also be trusted with global privileges in Identity Governance.

Separation of Duties Administrator

The Separation of Duties Administrator creates and manages SoD policies and violation cases.

8. Appendix B: Role Descriptions

The following 'Role Descriptions' are management functions and descriptions of their capabilities.

Access Request Approver

Access Request Approvers confirm whether to approve or deny requested access in the Request app. Identity Governance assigns this authorization if an Access Request Approval policy specifies approvers.

Application Owner

The Application Owner manages all assigned applications. This authorization can:

- View the catalog
- Perform data editing for assigned applications
- Review data and access within the assigned applications, depending on selections as a reviewer
- (Conditional) Review access entitlements or remediate access policy violations within the application if assigned this responsibility by the review definition

Application Administrator

The Application Administrator validates published data and performs data clean-up, or editing, for all assigned applications. This authorization can:

- Modify the configuration of a data source
- Execute collections for the data source
- Edit data within the scope of the data source
- Review data and access within the data source
- View the catalog but edit only items related to the assigned data source

Business Role Owner

The Business Role Owner can review a business role and potentially approve a business role depending on whether or not the assigned approval policy specifies Approved by owners. Business role owners cannot edit business roles, they can only view them.

Business Role Manager

A Business Role Manager can edit the assigned business roles, create, and delete new draft versions of the role but cannot delete the business role completely.

Escalation Reviewer

The Escalation Reviewer is an optional participant in a review. All tasks not completed on time are forwarded to the Escalation Reviewer for resolution. Otherwise, the tasks are forwarded to the Review Owner. This authorization can:

- View user, permission, application, and account details in the context of the review
- Decide whether to keep, modify, or remove access privileges for a user under review
- Edit review decisions before submitting those items

Fulfiller

The Fulfiller performs manual provisioning for access changes. This authorization can:

- View the changeset, identity, permission, and application details for each fulfillment request
- View guidance from collected analytics data about the requested change
- View the reason for the requested change and the source of the request, such as a review run, business role fulfillment, or SoD policy
- Fulfill, decline to fulfill, or reassign requests

Review Auditor

The Review Auditor authorization verifies a review campaign. Each review can have its own Review Auditor. This authorization can:

- Accept or reject the review after the Review Owner marks the review complete

- View the data related to the review but cannot modify the data

Review Owner

The Review Owner manages all assigned review instances. The Review Owner can view the details of any user, permission, or application entity within the context of the campaign. This authorization does not have general access to the catalog.

The Review Administrator who initiates a review automatically assumes the authorization of Review Owner if no Review Owner is specified.

NOTE: If you assign a new owner to a review, both the previous and new owners can access the review. The previous owner continues to see review instances run before the ownership change. The new owner sees only the instances run after the ownership change.

For an active Review, the Review Owner can:

- Start and monitor the review progress
- Resolve access policy violations in the review
- Reassign certification tasks within the review
- Run reports against the review
- Declare the review complete
- View review status in Overview
- View Quick Info details about a catalog item

Reviewer

The Reviewer authorization reviews sets of access permissions or memberships as part of a review run. This authorization can:

- Decide whether to keep, modify, or remove access privileges for a user under review
- Decide whether to keep or remove business role membership for a user under review
- Change the reviewer for any assigned review items
- View user, permission, application, and account details in the context of the review
- View a history of review decisions in the context of the review
- Edit review decisions before submitting them

SoD Policy Owner

The SoD Policy Owner is responsible for managing assigned Separation of Duties policies. This authorization can:

- Manage assigned policies
- Manage violation cases for assigned policies

9. Appendix C: Privilege to Role Mapping

Role	Assignment Method	Privilege
Access Request Approver	Access Request Approval policy	Access Request Administrator or Global Administrator
All global authorizations	**Administration** menu	Bootstrap administrator or Global administrator
Application Administrator	Application in the catalog	Application Owner, Data Administrator, Global Administrator, or Security Officer
Application Owner	Application in the catalog or review definition	Data Administrator, Global Administrator, or Security Officer
Business Role Manager	Business role definition	Business Roles Administrator, Global Administrator, or Security Officer
Business Role Owner	Business role definition	Business Roles Administrator, Global Administrator, or Security Officer
Escalation Reviewer	Review definition	Review Administrator or Global Administrator
Fulfiller	Application setup in **Fulfillment > Configuration** or Business Role definition	Business Roles Administrator Fulfillment Administrator, Global Administrator, or Security Officer
Permission Owner	Review definition	Global Administrator, Data Administrator, or Security Officer
Review Auditor	Review definition	Review Administrator or Global Administrator
Review Owner	Review definition	Review Administrator, Review Owner, or Global Administrator
Reviewer	Review definition	Review Administrator or Global Administrator
SoD Policy Owner	SoD policy definition	Separation of Duties Administrator or Global Administrator
Technical Role Owner	Technical role definition	Technical Roles Administrator or Global Administrator