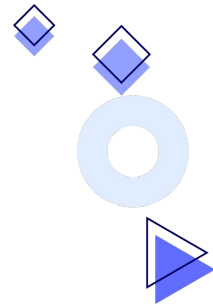




LAUREA MAGISTRALE INFORMATICA
Curriculum Cybersecurity



DB2 v12 for z/OS

Information Security Auditing, Certification and digital forensics

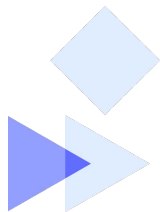
Studenti:

Luchini Chiara

Baldassarrini Matteo

Professore:

Milani Alfredo





Contenuti

01

Descrizione TOE

- DB2 e RAFC
- Struttura del TOE

02

Problemi di sicurezza

- Assunzioni
- Minacce
- Policy

03

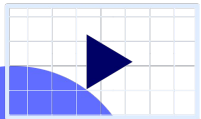
Obiettivi della sicurezza

- O
- OE
- Rationale

04

Requisiti della sicurezza

- SFRs
- SARs





Descrizione TOE





Descrizione del TOE

- Il TOE è l'applicazione software **DB2** e **RACF** stratificata su un sistema sottostante (che esegue z/OS V2.2):
 - **DB2** è un sistema multi-utente di gestione di database relazionali commercial-off-the-shelf (COTS) che opera come un sottosistema del sistema operativo, z/OS.
 - **RACF** (Resource Access Control Facility) è il componente centrale all'interno z/OS responsabile dell'autenticazione dell'utente, del controllo dell'accesso, della gestione degli attributi di sicurezza dell'utente e dei diritti di accesso.

Executive summary

TOE nome: DB2 v12 for z/OS

Sponsor: IBM Corporation ®

Sviluppatore: IBM Corporation

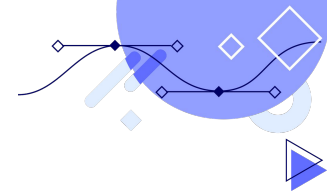
Evaluation Assurance Level: EAL4

augmented with ALC_FLR.3

CC version: 3.1 Rev. 4

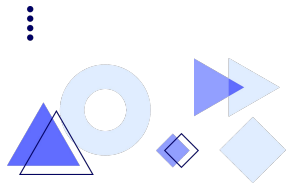
Evaluation starting date: 2 Maggio 2017

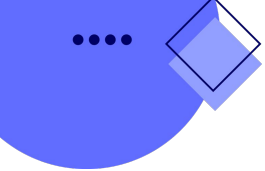
Evaluation ending date: 16 Ottobre 2017



TOE Architecture: Hardware

- Il **DB2** v12 funziona come un sottosistema all'interno del sistema operativo z/OS V2R2. Quindi, la piattaforma di runtime richiesta per esso è la stessa del sistema operativo.
- Il TOE viene eseguito all'interno di una **partizione logica** fornita da una versione certificata di PR/SM, su z/Architecture sviluppate da IBM.
- Inoltre il TOE può essere eseguito in una **macchina virtuale** fornito da una versione certificata di z/VM.





TOE Architecture: Software

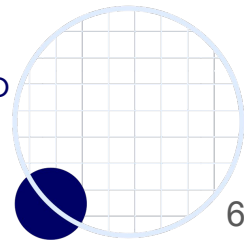
DB2 è implementato da un insieme **di spazi di indirizzo** più un insieme di **utilities**.

Gli utenti possono accedere a DB2 localmente usando "**attachment facilities**" o remotamente tramite la **Distributed Data Facility** che usa i protocolli DRDA. Le strutture di collegamento vengono eseguite nello spazio degli indirizzi del chiamante e comunicano con gli spazi degli indirizzi del DB2 per servire le richieste dell'utente.

Le strutture di collegamento includono:

- la struttura di collegamento **TSO** (Time Sharing Option).
- la **Call Attachment Facility (CAF)**, che permette ai programmi in esecuzione sotto TSO o nell'ambiente batch z/OS di comunicare con il DB2.
- La **Resource Recovery Services Attachment Facility (RRSAF)** è un'implementazione più recente di CAF con capacità aggiuntive.
- Infine gli utenti che accedono in remoto tramite **DRDA** si connettono a un server di applicazioni o a un server di database.

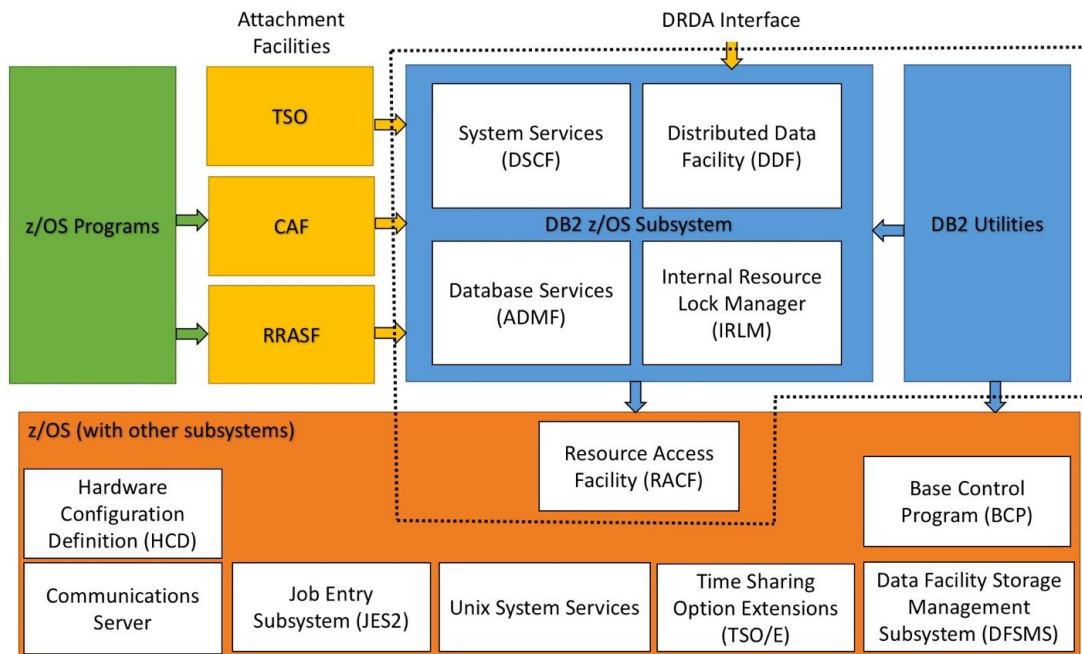
Le **DB2 Utilities** sono un insieme di programmi online e standalone che forniscono funzioni di diagnostica e manutenzione del database per gli amministratori.



Struttura base

La seguente figura mostra la **struttura** di base di DB2 e le strutture di collegamento supportate nella configurazione valutata, i diversi box in base al colore rappresentano:

- Rappresentano le parti “trusted” del DB2
- Indicano le strutture di collegamento
- Rappresenta il sistema z/OS come piattaforma del TOE
- Rappresenta i programmi utente “untrusted” usati dai servizi di z/OS
- ... Mostrano i limiti del TOE



Problemi di sicurezza



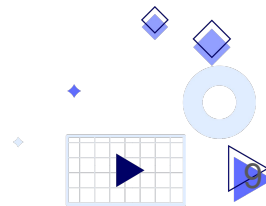
Problemi di sicurezza: introduzione

Nelle slides successive andremo a descrivere le caratteristiche di sicurezza dell'ambiente in cui il TOE viene usato.

A tal proposito saranno riportate delle liste di:

- **assunzioni** formulate sull'ambiente operativo;
- **minacce** che il prodotto riesce a contrastare;
- **policy di sicurezza organizzative** alle quali il prodotto è conforme.

In questo **Security Target** sono presenti solo tutte le assunzioni, minacce e policy di sicurezza organizzativa definite nelle diverse sezioni del **Protection Profile per DBMS**.



Assunzioni 1/2

01. A.PHYSICAL

Si presume che l'ambiente IT fornisca al TOE una sicurezza fisica adeguata, commisurata al valore dei beni informatici protetti dal TOE

02. A.AUTHUSER

Gli utenti autorizzati possiedono l'autorizzazione necessaria per accedere ad almeno alcune delle informazioni gestite dal TOE.

03. A.SUPPORT

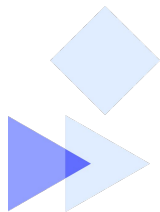
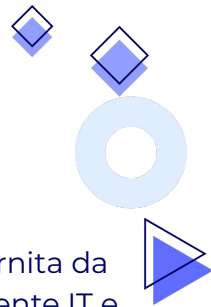
Qualsiasi informazione fornita da un'entità fidata nell'ambiente IT e utilizzata per supportare la fornitura di ora e data, informazione molto importante che viene utilizzata dal TOE è corretta e aggiornata

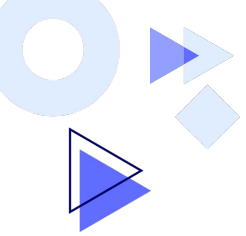
04. A.TRAINEDUSER

Gli utenti sono sufficientemente addestrati e fidati per svolgere diversi compiti all'interno di un ambiente informatico sicuro, esercitando un controllo completo sui loro dati utente.

05. A.MANAGE

La funzionalità di sicurezza del TOE è gestita da uno o più individui competenti. Il personale amministrativo del sistema non è disattento, intenzionalmente negligente o ostile, e seguirà e rispetterà le istruzioni fornite dalla documentazione di guida.





Assunzioni 2/2



06. A.PEER_FUNC_&_MGT

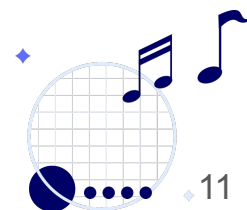
Tutti i sistemi IT remoti di cui il TSF si fida si presume che implementino correttamente la funzionalità utilizzata dal TSF in modo coerente con i presupposti definiti per questa funzionalità e che siano gestiti correttamente e operino sotto vincoli di politica di sicurezza compatibili con quelli del TOE.

07. A.NO_GENERAL_PURPOSE

Non sono disponibili capacità di calcolo di uso generale sui server DBMS, oltre a quei servizi necessari per il funzionamento, l'amministrazione e il supporto del DBMS.

08. A.CONNECT

Tutte le connessioni da/e verso sistemi IT remoti fidati e tra parti separate del TSF sono fisicamente o logicamente protette all'interno dell'ambiente TOE per assicurare l'integrità e la riservatezza dei dati trasmessi e per garantire l'autenticità dei punti finali della comunicazione.



Minacce 1/2



01.

T.ACCESS.TSFDATA

Un agente malevolo può leggere o modificare i dati TSF utilizzando le funzioni del TOE senza la corretta autorizzazione.

02.

T.ACCESS.TSFFUNC

Un agente malevolo può utilizzare o gestire TSF, aggirando i meccanismi di protezione del TSF.

03.

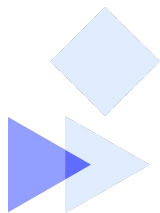
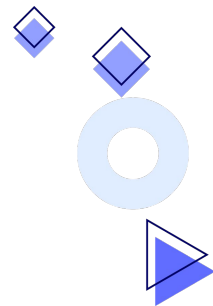
T.IA.MASQUERADE

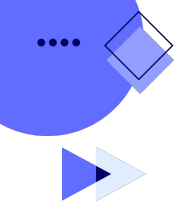
Un utente o un processo può mascherarsi da un'entità autorizzata al fine di ottenere l'accesso non autorizzato ai dati dell'utente, ai dati TSF o alle risorse TOE.

04.

T.IA.USER

Un agente malevolo può accedere ai dati dell'utente, ai dati TSF o alle risorse TOE con l'eccezione di oggetti pubblici senza essere identificati e autenticati.





05.

T.RESIDUAL_DATA

Un utente o un processo che agisce per conto di un utente può ottenere l'accesso non autorizzato ai dati di utente o TSF attraverso la riallocazione delle risorse TOE da un utente o processo a un altro.

06.

T.TSF_COMPROMISE

Un utente o un processo che agisce per conto di un utente può accedere inappropriatamente ai dati di configurazione o può compromettere il codice eseguibile del TSF.

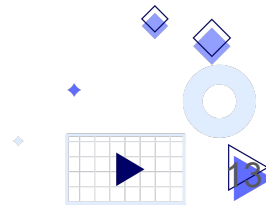
Minacce 2/2



07.

T.UNAUTHORIZED_ACCESS

Un agente malevolo può ottenere l'accesso non autorizzato ai dati degli utenti.



Policy di sicurezza

01.

P.ACCOUNTABILITY

Gli utenti autorizzati del TOE sono ritenuti responsabili delle loro azioni all'interno del TOE.

02.

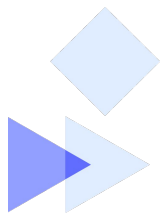
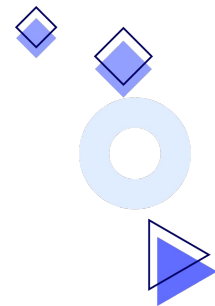
P.ROLES

L'autorità amministrativa per la funzionalità del TSF deve essere conferita a personale di fiducia ed essere il più limitata possibile supportando solo i compiti amministrativi che la persona ha. Questo ruolo deve essere separato e distinto dagli altri utenti autorizzati.

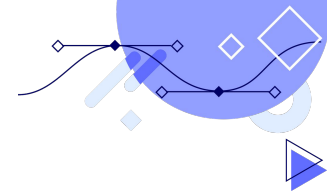
03.

P.USER

L'autorizzazione deve essere concessa solo agli utenti che sono affidabili per eseguire correttamente le azioni.



Obiettivi della sicurezza



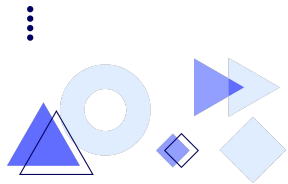
Obiettivi della sicurezza: introduzione

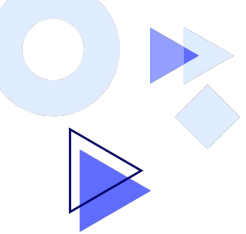
Nelle prossime slides verranno descritti i diversi **obiettivi di sicurezza** che hanno come scopo quello di contrastare le minacce individuate rispettando le assunzioni e policy di sicurezza viste in precedenza.

Questi obiettivi sono divisi in 2 categorie:

- **Security Objectives for the TOE (O)**
- **Security Objectives for the Operational Environment (OE)**

Tutti gli obiettivi che saranno descritti sono solo quelli presenti all'interno delle rispettive sezioni nel **Protection Profile per DBMS**.





Security Objective for the TOE 1/2

01. O.ADMIN_ROLE

Il TOE fornirà un meccanismo mediante il quale le azioni che utilizzano privilegi amministrativi possono essere limitate.

02. O.I&A

Il TOE assicura che gli utenti siano autenticati prima che il TOE elabori qualsiasi azione che richieda autenticazione.

03. O.MEDIATE

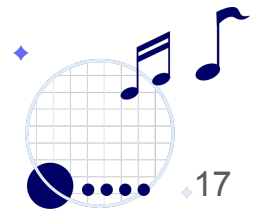
Il TOE deve proteggere i dati degli utenti in conformità con la sua politica di sicurezza e deve mediare tutte le richieste di accesso a tali dati.

04. O.AUDIT_GENERATION

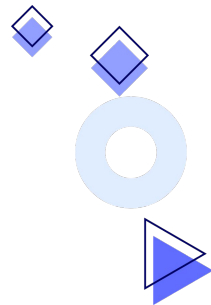
Il TSF deve essere in grado di registrare eventi definiti rilevanti per la sicurezza con data e ora identificando l'utente che ha causato tale evento. Il tutto deve essere sufficientemente dettagliato per far rilevare agli utenti autorizzati eventuali tentativi di violazione o configurazioni errate delle caratteristiche di sicurezza del TOE.

05. O.ACCESSO_DISCREZIONALE

Il TSF deve controllare l'accesso di utenti a risorse denominate in base all'identità dell'oggetto. Il TSF deve permettere agli utenti autorizzati di specificare per ogni modalità di accesso quali utenti sono autorizzati ad accedere a uno specifico oggetto denominato in quella modalità di accesso.



Security Objective for the Toe 2/2



06. O.MANAGE

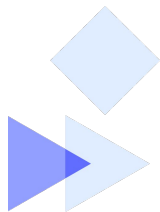
Il TSF deve fornire tutte le funzioni e le strutture necessarie per supportare gli utenti autorizzati che sono responsabili della gestione dei meccanismi di sicurezza del TOE permettendone la limitazione a utenti dedicati e deve garantire che siano in grado di accedere alle funzionalità di gestione.

07. O.TOE_ACCESS

Il TOE fornirà la funzionalità che controlla l'accesso logico di un utente ai dati dell'utente e al TSF.

08. O.RESIDUAL_INFORMATION

Il TOE assicura che qualsiasi informazione contenuta in una risorsa protetta all'interno del suo ambito di controllo non venga divulgata in modo inappropriato quando la risorsa viene riassegnata.



Obiettivi di sicurezza OE 1/2



01.

OE.ADMIN

I responsabili del TOE sono persone competenti e affidabili, in grado di gestire il TOE e la sicurezza delle informazioni in esso contenute.

02.

OE.INFO_PROTECT

I responsabili del TOE devono stabilire e attuare procedure per assicurarsi che le informazioni siano protette in modo appropriato.

03.

OE.NO_GENERAL_PURPOSE

Non ci saranno capacità di calcolo generiche disponibili sui server DBMS, diversi dai servizi necessari al funzionamento, amministrazione e supporto del DBMS.

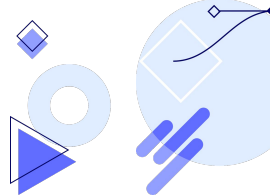
04.

OE.PHYSICAL

I responsabili del TOE devono assicurare che le parti critiche di quest'ultimo siano protette da attacchi fisici che possono compromettere gli obiettivi di sicurezza del IT.



Obiettivi di sicurezza OE 2/2



05.

OE.IT_I&A

Qualsiasi informazione fornita da un'entità fidata nel sistema e utilizzata per supportare l'autenticazione dell'utente e l'autorizzazione usata dal TOE è corretta e aggiornata.

07.

OE.IT_TRUSTED_SYSTEM

I sistemi IT affidabili remoti implementano i protocolli e i meccanismi richiesti dal TSF per supportare l'applicazione della politica di sicurezza. Questi sistemi sono gestiti in base a politiche note, accettate e affidabili basate sulle stesse regole e politiche applicabili al TOE, e sono fisicamente e logicamente protetti.

06.

OE.IT_REMOTE

Se il TOE si affida a sistemi IT remoti “trusted” per supportare l'applicazione della sua politica, tali sistemi prevedono che le funzioni e gli eventuali dati utilizzati dal TOE sono sufficientemente protetti da qualsiasi attacco che possa portare a risultati falsi di tali funzioni.





Rationale for TOE Security Objectives

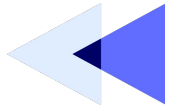
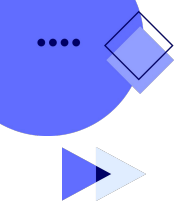


	T.ACCESS.TSF DATA	T.ACCESS.TS FFUNC	T.IA.MASQUER ADE	T.IA.USER	T.RESIDUAL_ DATA	T.UNAUTHORI ZED_ACCES	T.TSF_COMPR OMISE
O.ADMIN_ROLE		X					
O.AUDIT_GENERATION							X
O.DISCRETIONARY_ACCESS				X		X	
O.I&A	X	X	X	X			
O.MANAGE	X	X				X	
O.MEDIATE			X	X		X	
O.RESIDUAL_INFORMATION	X	X			X		
O.TOE_ACCESS	X	X	X	X			X

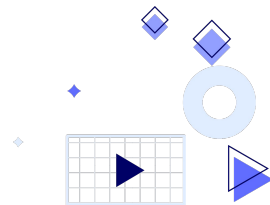
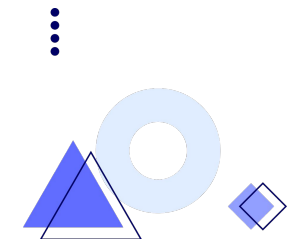


Rationale for the Environmental Security Objectives

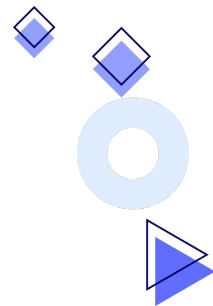
	A.PHYSICAL	A.AUTHUSER	A.SUPPORT	A.TRAINEDUSER	A.MANAGE	A.PEER_FUNC_ &_MGT	A.NO_GENERAL _PURPOSE	A.CONNECT	T.ACCESS.TSFD ATA	T.ACCESS.TSFF UNC	T.MASQUERADE	T.IA.USER	T.RESIDUAL_DA TA	T.UNAUTHORIZED _ACCESS	T.TSF_COMPRO MISE
OE.ADMIN					X										
OE.INFO_PROTECT	X	X		X	X			X						X	X
OE.IT_I&A			X												
OE.IT_REMOTE		X				X		X							X
OE.IT_TRUSTED_SYSTEM		X				X		X							X
OE.NO_GENERAL_ PURPOSE							X				X				X
OE.PHYSICAL	X							X							X ₂₂



SFR e SAR



Security Requirements: SFR



Per concludere, andiamo ad analizzare gli **SFR** e **SAR** soddisfatti dal TOE in base agli obiettivi visti in precedenza.

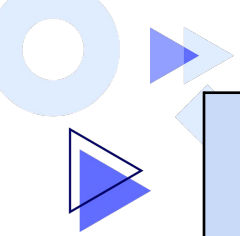
Questi requisiti comprendono i **functional requirement** della Parte II del Common Criteria e gli **assurance components** della parte III del CC, con l'aggiunta del componente **ALC_FLR.3**.

Possiamo suddividere gli SFR nelle seguenti sottocategorie:

- Security Audit (**FAU**);
- Cryptographic Support (**FCS**);
- User Data Protection (**FDP**);
- Identification & Authentication (**FIA**);
- Security Management (**FMT**);
- Protection of the TSF (**FPT**).

Nelle seguenti slides vedremo tutti gli SFR associati ai vari obiettivi citati in precedenza.





	SFR	
	FMT_SMR.1	FDP_RIP.1
Obiettivo		
O.ADMIN_ROLE	x	
O.RESIDUAL_INFORMATION		x

FMT_SMR.1 - Security Roles

Comprende 2 componenti:

- **FMT_SMR.1.1** - Il TSF mantiene i ruoli
- **FMT_SMR.1.2** - Il TSF deve essere in grado di associare gli utenti ai ruoli

Razionale

Il TOE stabilirà almeno un ruolo di amministratore autorizzato, che avrà i privilegi per eseguire specifici compiti come l'accesso alle informazioni di controllo e funzioni di sicurezza. L'autore della ST può scegliere di specificare più ruoli.

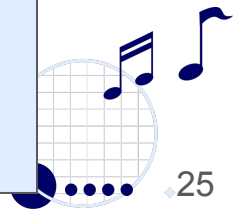
FDP_RIP.1 - Subset residual information protection

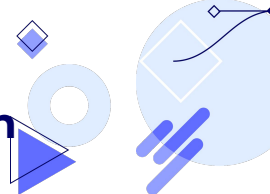
Comprende 1 componente:

- **FDP_RIP.1.1** - Il TSF assicura che qualsiasi contenuto informativo precedente di una risorsa sia reso indisponibile.

Razionale

FDP_RIP.1 è usato per assicurare che quando un DB2 viene cancellato, lo spazio che era occupato non possa essere accessibile dalle funzioni TOE.






Obiettivi	SFR
O.AUDIT_GENERATION	<ul style="list-style-type: none">• FAU_GEN.1• FAU_GEN.2• FAU_SEL.1

FAU_SEL.1 - Selective audit

Il TSF deve essere in grado di selezionare l'insieme di eventi da sottoporre a audit dall'insieme di tutti gli eventi verificabili in base a diversi attributi.

Razionale

Il TOE supporta una selezione di eventi possono essere controllati in base a una serie di attributi.



FAU_GEN.1 - Audit data generation

Il TSF deve essere in grado di generare un record di audit in base a diversi eventi definiti nel ST.

Razionale


Gli eventi da controllare in DB2 sono definiti in FAU_GEN.1 e sono associati all'identità dell'utente che ha causato l'evento.

FAU_GEN.2 - Audit data generation

Il TSF deve registrare all'interno di ogni record di audit almeno le informazioni presenti nel ST.

Razionale

Usato FAU_GEN.2 per l'audit trail che risulta dalle azioni del RACF e FAU_GEN.2 per il DB2 audit trail.



Obiettivo	SFR		
	FDP_ACF.1	FDP_ACC.1	FPT_TRC.1
O.DISCRETIONARY.ACCESS	x	x	
O.MEDIATE	x	x	x

FDP_ACC.1 - Subset access control

Comprende 1 componente:

- **FDP_ACC.1.1** - Il TSF applica la politica di Discretionary Access Control agli oggetti su tutti i soggetti, tutti gli oggetti controllati da DBMS e tutte le operazioni tra di essi.

Razionale per O.MEDIATE

FDP_ACC.1 definisce la politica di Access Control che verrà applicata su un elenco di soggetti che agiscono per conto di altri utenti che tentano di ottenere l'accesso a un elenco di oggetti con nome.

FPT_TRC.1 - Internal TSF consistency

Comprende 2 componenti:

- **FPT_TRC.1.1** - Il TSF assicura che i dati siano coerenti quando vengono replicati tra le parti del TOE.
- **FPT_TRC.1.2** - il TSF assicura la coerenza dei dati al momento della riconnessione tra parti del TOE.

Razionale

FPT_TRC.1 garantisce che i dati TSF replicati che specificano gli attributi per il controllo di accesso devono essere coerenti tra le componenti distribuite dell'EPT.



FMT_MSA.3 - Static attribute initialization

Comprende due componenti:

- **FMT_MSA.3.1:** Il TSF applicherà la politica di controllo dell'accesso discrezionale per fornire valori predefiniti di errore per gli attributi di sicurezza utilizzati per applicare SFP.
- **FMT_MSA.3.2:** Il TSF non consente a nessun utente di specificare valori iniziali alternativi per sovrascrivere i valori predefiniti quando viene creato un oggetto o un'informazione.

Obiettivi	SFR
O.MANAGE	<ul style="list-style-type: none">• FMT_MOF.1• FMT_MSA.1• FMT_MSA.3• FMT_MTD.1• FMT_REV.1(1)• FMT_REV.1(2)• FMT_SMF.1• FMT_SMR.1

Razionale

FMT_MSA.3 richiede che i valori predefiniti utilizzati per gli attributi di sicurezza siano restrittivi.

FMT_MSA.1 - Management of security attributes

Il TSF applicherà la politica di Discretionary Access Control per limitare la capacità di gestire tutti gli attributi di sicurezza agli amministratori autorizzati.

Razionale

FMT_MSA.1 richiede che la capacità di eseguire operazioni sugli attributi di sicurezza sia limitata a ruoli particolari.

Obiettivo	SFR							
	FIA_ATD.1	FIA_UID.1	FIA_UAU.1	FIA_USB_(EXT).2	FDP_ACC.1	FDP_ACF.1	FTA_MCS.1	FTA_TSE.1
O.I&A	x	x	x	x				
O.TOE_ACCESS	x				x	x	x	x

FIA_ADT.1 - User attribute definition

Ha una singola componente **FIA_ADT.1.1** che indica che Il TSF mantiene il seguente elenco di attributi di sicurezza appartenenti ai singoli utenti:

- Identificatore degli utenti del DB
- Ruoli del database rilevanti per la sicurezza
- Lista di attributi di sicurezza

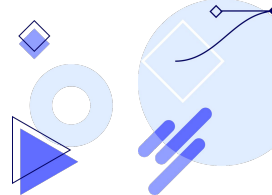
Razionale per O.I&A

Gli attributi di sicurezza usati per determinare l'accesso sono definiti e disponibili al supporto delle decisioni di autenticazione come richiesto da **FIA_ATD.1**.

Razionale per O.TOE_ACCESS

Definisce gli attributi di sicurezza per i singoli utenti, gli attributi di sicurezza rilevanti e altri attributi di sicurezza dell'identità.

Security requirements: SAR



Identificano le attività di gestione e di valutazione necessari per affrontare le minacce e le politiche individuate precedentemente.

Queste classi vengono suddivise in:

- Development (**ADV**);
- Guidance Documents (**AGD**);
- Testing (**ATE**);
- Vulnerability Assessment (**AVA**);
- Life cycle support (**ALC**);
- Security Target evaluation (**ASE**);

I requisiti di garanzia della sicurezza per il TOE corrispondono al **Evaluation Assurance Level 4**, aumentato da **ALC_FLR.3**, come specificato nel CC parte 3. Inoltre, il livello di garanzia della valutazione è coerente con il **minimo assurance level (EAL 2)** in [DBMSPP].

EAL4: metodicamente progettato, testato e rivisto.

Si applica quando gli sviluppatori o gli utenti richiedono una sicurezza garantita, in modo indipendente, da moderata a elevata nei prodotti di base convenzionali e sono disposti a sostenere costi di progettazione specifici per la sicurezza aggiuntiva.



EAL2



I CC prevedono una classe di assurance (6 componenti, 6 famiglie) per la valutazione di **Protection Profile** ed una classe di assurance (8 componenti, 8 famiglie) per la valutazione di **Security Target**.

Nel nostro caso usiamo la classe **Security target evaluation (ASE)**, la quale non compare nei package EAL predefiniti.

L'obiettivo di questa famiglia è descrivere il TOE in modo narrativo con tre livelli di astrazione: **riferimento TOE**, **panoramica TOE** e **TOE descrizione**.

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle 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.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification

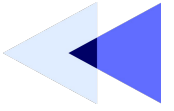
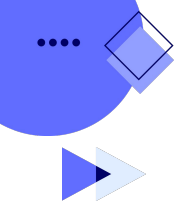
ALC_FLR.3

Systematic flaw remediation

Obiettivi

Affinché lo sviluppatore possa agire in modo appropriato in caso di segnalazioni di falle di sicurezza dagli utenti del TOE, e per sapere a chi inviare correzioni correttive, gli utenti del TOE devono capire come inviare segnalazioni di falle di sicurezza allo sviluppatore, e come comunicare con lo sviluppatore in modo che possano ricevere queste correzioni correttive. La guida alla correzione dei difetti dallo sviluppatore all'utente del TOE garantisce che gli utenti siano a conoscenza di queste importanti informazioni.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4



**Grazie per
l'attenzione!**

