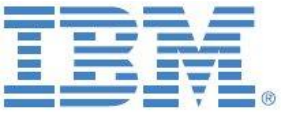

IBM Planning Analytics
Proven Practices for
Security Management and Auditability

Prepared:
May 2017

Created By:

Andreas Kugelmeier
Executive Consultant, FOPM
Planning Analytics Architect
IBM Data and AI Expert Labs
Mobile Phone: +1-215-384-7302
Email: kugelmeier@us.ibm.com

Notices & Disclaimers

Information in these presentations and papers (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS document is distributed "AS IS" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity. IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.
Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.
Performance data contained herein was generally obtained in a controlled, isolated environment. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.
Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose.
The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.
- The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

Document Version History

Date	Version	Author	Description
5/15/2017	1.0	Andreas Kugelmeier	

Table of Contents

1 Auditability & Automation via mapping of Functional User-Roles to TM1 security groups

By creating a granular taxonomy of Financial Analytics & Performance Management User Roles and Definitions, mapping rules can be created that can automatically align the user roles (via their corresponding AD groups) to corresponding TM1 object security credentials. *Without* a granular User-Role taxonomy and associated AD user groups, individual user roles/profiles would have to be mapped to TM1 Object-security via manual intervention. This would occur by either creating TM1 Object-based security groups and mapping user profiles to TM1-object security groups or via role-based TM1 security groups which would be mapped implicitly to TM1 object security:

	Object-based Security Groups	***Role-based TM1 Security Groups***
Advantages	High technical transparency into granted security credentials	Fast ad-hoc deployment of new security profiles/roles (but: high maintenance effort for changes)
Disadvantages	Manual mapping of • user roles (functional) to • object based (technical) groups is required. resulting in • significant security maintenance efforts • significantly reduced auditability & traceability of a user's TM1 access credentials outside of TM1 • security vulnerabilities due to manual errors	Manual mapping of • user roles (functional) to • object based (technical) groups is required. resulting in • significant security maintenance efforts • significantly reduced auditability & traceability of a user's TM1 access credentials outside of TM1 • security vulnerabilities due to manual errors

In both cases, the mapping of the users' security profiles (the roles) to TM1 security must occur manually:

?

					TM1 User Groups									
	User Role Descriptions				**Functional and/or Object-based Groups**									
	...	**...**	**...**	**...**	**Cube A**	**Cube B**	**...**	**Dim A**	**Dim B**	**...**	**Group A**	**Group B**	**...**
User A	X		X		X	X			X			X	
User B		X	X			X	X			X	X	X	
User C			X				X			X	X		X

To automate this manual process and to achieve and sustain highest reliability and auditability of granted security within the TM1 environment, it is a recommended practice to develop a granular User-Role taxonomy and corresponding User Roles. The resulting User Roles, once created in AD and using AD-integrated by TM1, allow the automated mapping of Business-***Functional User Roles*** to ***Object-based Security Groups*** in the TM1 security management instance:

	RECOMMENDED: business-functional User Roles/Groups, mapped to *Security Groups*
Advantages	• High transparency into granted security credentials (from a technical perspective) • High Auditability & Traceability of security access credentials • Security Automation via **Automated Mapping of Business-functional User Roles to Object-based security groups**

Automated Mapping

	TM1 User Groups														
	Business-Functional User Role Groups (created in AD)					**Functional and/or Object-based Groups**									
	UK Analyst Type I	**UK Analyst Type II**	**...**	**UK Planner Type I**	**...**	**Cube A**	**Cube B**	**...**	**Dim. A**	**Dim. B**	**...**	**Group A**	**Group B**	**...**
User A	X		X	X		X	X			X			X	
User B		X	X	X			X	X			X	X	X	
User C		X						X			X	X		X

Via the mapping of Business-Functional User Roles to 'Object-based Security', the disadvantages of the '*Object-based Security Group*' approach as per the above table will dissipate. Specific Benefits:

- Full auditability and traceability of TM1 User access credentials (due automation of the relationship between User Roles and Object Groups)
- Significantly Reduced Maintenance efforts (security management can largely be automated)

The *business-functional user roles* themselves would each become a TM1 Security Group, resulting in two types of security groups in TM1: **(A) Functional user groups & (B) Object-level security groups**. TM1 Security access credentials would still be defined against the object-level security groups. No access credentials would be granted to a Functional User Group alone. Instead, a user's assignment to TM1 object security groups would occur automated, based on the functional user groups the user belongs to. The translation from User Role(s)/Groups (business view) to Object-based Groups (technical view) would occur automatically in the TM1 security management instance.

2 Synchronization between AD/DW and IBM Planning Analytics

If security metadata is available in an active directory or DW, it should be leveraged by IBM Planning Analytics, i.e. if for example a DW/AD contains security metadata on groups, dimensions, hierarchies and dimension elements/members that pertain to dimensions and hierarchies used by the IBM Planning Analytics solutions infrastructure, this security metadata should be pulled from the DW/AD and applied to TM1 automatically.[1]

[1] If in DW: Via an ODBC connection to DW Security Metadata tables & ideally using Cognos Command Center as the automation orchestration and management tool for Security Metadata synchronization tasks
If in AD: via ETLDAP extraction

3 Data Security Management & Maintenance

Options for TM1 Data Security Management & Maintenance:

	disadvantages	advantages
TM1 UI	• cumbersome to use, especially for element level security on larger dimensions with many hierarchy levels; • no automation	• built-in UI (with very basic functionality)
Directly against TM1 Security Cubes	• cumbersome to use, especially for element level security on larger dimensions with many hierarchy levels; • no automation	• can use cube views, PAX, PAW
Security Maintenance Model	Not built-in, but an IBM plug&play model is available on demand	• can use cube views, PAX, PAW • semi-automated to fully automated security maintenance updates • fast performance, especially when targeting specific security groups/roles, and specific objects (dimensions) that are to be updated • re-configuration can be wide-ranging/far-reaching without having to be applied to TM1 model => apply new security only when ready • easier configuration for hierarchy based element security • ability to target specific security areas/ groups only (speed)

To streamline the setup, management & maintenance of TM1 object & data security in any larger analytics environment that is leveraged by many users and with sufficiently high volatility (new users, retirement of users, changing security profiles, …), it is recommended to deploy a TM1 Security Management & Maintenance Framework