Ray - SoD app
General Agreement

expertum

Contents

1 Introduction

The General Agreement for Ray describes the content of a subscription to Ray. Besides the subscription itself, it also describes the possible optional services related to Ray. The General Agreement is the global agreement between Expertum and the customer.

The price quote to subscribe to Ray and to buy optional services will be appended to this document in separate workorders.

2 Description of RAY

2.1 On what platform does Ray operate?

Ray brings you SOD as a Service (SaaS). Ray is built on the latest SAP BTP technology and uses the power of HANA. To perform his analyses, Ray needs a fair amount of computing power. The BTP technology and the HANA database provide this necessary computing power. By subscribing to Ray, you'll get the required runtime capacity on the SAP BTP platform to have Ray operate smoothly.

Technically, our application and all its related customer data is deployed and stored on SAP BTP. Expertum is consuming BTP services from SAP and has chosen to deploy those services on Microsoft Azure with data center in the Netherlands. This ensures that all GDPR rules are applicable and applied. Moreover, the fact that Expertum consumes services from SAP on an SAP BTP platform, the **SAP's General Terms and Conditions for Cloud Services** (Appendix 1) fully apply to Ray.

When subscribing to Ray, Expertum provides the customer with a private tenant on the SAP BTP platform accessible through a private URL. This private tenant ensures that all customer data is secured and separated from other customer's data using Ray. Refer to Appendix 2 for the **Expertum Terms and Conditions**.

Expertum will provide access to the necessary Ray users on the private tenant of the customer. The following types of users exist:

- **Basic User**: This type of user can display everything Ray does (run lists, dashboards, evolutions, remediation progress, etc.)
- **Risk Analyst**: This type of user has the same accesses as the basic user, but the accesses are extended to execute risk analysis runs.
- **Administrator**: This type of user has the same accesses as the risk analyst, but the accesses are extended to: maintain systems and system data, maintain run parameters and remove (obsolete) data.

2.2 What does Ray do?

SAP Authorizations are a complex matter. Although they can be a strong preventative control, getting your critical accesses and segregation of duties (SOD) under control usually is a difficult task. Expertum has developed Ray, your virtual Security Officer, to **identify** and **visualize** your SAP authorizations risks and to support your **remediation activities**.

Ray has the following features:

- **Risk Identification**
  - The risk identification engine runs on **user level** and on **role level** (single / derived / composite role level).
  - The engine uses a **detailed ruleset** down to the level of authorization objects, fields and field values.
  - Both **critical access** and **segregation of duties** (SOD) risks are covered.
  - Traditional **transaction codes**, **WebDynpros** and **UI5 Fiori apps** are all covered by the engine / ruleset.
  - The app runs on every **NetWeaver based SAP system with PFCG-based roles**, including SAP ECC, S/4HANA on-premise and S/4HANA on Rise.
- **Risk Visualisation**
  - The risk results are visualised through **clear dashboards**, making the sometimes complex results understandable for a broad audience
- **Risk Remediation**
  - The complex **remediation process is supported** by visualising the new, open, approved, remediated, and mitigated risks as you progress in your remediation actions.

2.3 What ruleset does Ray use?

To operate, Ray needs detailed ruleset down to the level of authorization objects, fields and field values. Out of the box, Ray brings a small starter ruleset with him. This ruleset allows Ray to at least start operating. This starter ruleset contains:

- 16 Critical Access rules
- 1 Critical Permission rule
- 17 Segregation of Duties rules

However, to allow Ray to perform his job to the fullest, a more elaborate and customized ruleset is required. Refer to §4 to learn how Expertum can help you establish your full blown ruleset.

2.4 How will Ray be updated?

New features will be added regularly to the Ray software. Expertum will push these new features regularly to the customer's tenant. These new features will be communicated clearly and on a timely manner and will be demoed on request.

2.5 How will Ray be supported?

Ray does not operate on his own. Expertum is supporting him in his operations. From within the Ray application, tickets can be raised towards Expertum with questions, bugs (if any), requests for changes and additions, etc. For changes and additions, Expertum reserves the right to evaluate them and to decide whether or not to implement the requested change.

3 License Model and Subscription Fee

3.1 1-Time Setup Cost

For getting Ray to work, there are some 1-time things to be setup on the BTP platform:

- Setup and provision of the subaccount for the customer
- Define and authorize the needed users from the customer that will work with Ray
- Setup and configure Expertum's ticketing system allowing the customer to create support tickets from within the RAY application
- Implement the Ray download ABAP on the customer's landscape(s). Ray needs a set of user and authorizations related tables to operate. This ABAP enables the customer to automate the table downloading from the systems.
- End-User Training

3.2 Subscription Model

The subscription model consists of 2 parts:

- **License part**: The metric for this part is blocks of 100 monitored users. A monitored user is defined as a user-ID that is considered by Ray during a dashboard run. In case Ray is monitoring multiple systems / landscapes, unique user-IDs are taken into account. If a particular user-ID is considered in 3 different systems, for example, this is counted as 1 monitored user. The price per block of 100 monitored users decreases with the size of your systems.
- **Runtime part**: The larger your system data, the more computing power Ray needs to run your analyses. Therefore, the runtime cost increases with the size of your systems.

The subscription model(*) is shown in the below table:

Blocks		Per month		
From	To	License/Block	Runtime	Model
1	5	€ 96,00	€ 239,72	Low
6	10	€ 80,00	€ 261,15	Medium
11	15	€ 64,00	€ 261,15	Medium
16	25	€ 48,00	€ 271,98	High
26	35	€ 32,00	€ 271,98	High
36	45	€ 16,00	€ 293,02	Very High
46	999	€ 0,00	€ 293,02	Very High

(*) illustrative cost per license block & runtime

The different runtime models are:

Blocks	Memory	Compute	Storage
Low	64Gb	8vCPU	200Gb
Medium	96Gb	12 vCPU	280Gb
High	128Gb	16vCPU	360Gb
Very High	256Gb	32vCPU	680Gb

3.3 Calculation example

Assume the customer has 1.650 monitored users. Applying the subscription model, the customer then needs 17 license blocks. This results in the following subscription price:

From 1/1/2025 till 31/12/2025

Product	Usage Metric (# Blocks of 100 Users)	Runtime model	List Price / Month	List Price / Year
Ray - Your virtual SOD Officer	17	High: 128Gb RAM / 16 vCPU / 360Gb	€ 1.567,98	€ 18.815,75

Yearly Discounted Subscription Price		**€ 18.815,75**
1-Time Setup Cost		**€ 3.000,00**
VAT	21%	€ 4.581,31
Total (incl. VAT)		**€ 26.397,06**

The detailed subscription price calculation is as follows:

Blocks	Calculation	List Price / Month
1 to 5	5 * € 96	€ 480,00
6 to 10	5 * € 80	€ 400,00
11 to 15	5 * € 64	€ 320,00
16 to 17	2 * € 48	€ 96,00
Runtime	High: 128Gb RAM / 16 vCPU / 360Gb	€ 271,98
		€ 1.567,98

4 Ruleset Consulting (Optional)

Out of the box, Ray brings a starter ruleset with him to at least start operating. However, to allow Ray to perform his job to the fullest, a more elaborate and customized ruleset is required.

Over the past 15 years, Expertum has developed an extensive ruleset containing:

- 309 Critical Access rules
- 224 Critical Permission rule
- 893 Segregation of Duties rules

In order to establish a full monitoring ruleset for the customer, this Expertum ruleset can optionally be used as a starting point. The **enhancements** to be done on the Expertum ruleset to make it a customer specific version are:

- Activating / deactivating risks depending on your implemented business processes, control requirements and risk appetite.
- Adding own developed transaction codes, WebDynpro applications and/or Fiori apps.
- Adding own developed authorization objects and implemented own authority checks.
- Adapting the risk severity in the ruleset depending on your implemented business processes, control requirements and risk appetite.

To use and customize the extensive Expertum ruleset the following applies:

- To use the Expertum ruleset as a starting point, a **1-time ruleset fee** applies.
- Our regular Senior Consultant rates apply for assisting you in further enhancing the ruleset as just described. The **scope and extent** of these enhancements can be determined in **mutual agreement**.

In case you would already have an **internal ruleset** in some digital format, Expertum can convert that ruleset to the required **Ray ruleset format**, as well. In this case, our regular Senior Consultant rates apply to the **conversion** work needed. Without further enhancements to that internal ruleset, the conversion work is estimated to **2 to 5 man-days**, depending on the size of the ruleset and on how big the format delta is between the internal ruleset and the Ray ruleset format.

5 Proof of Concept (Optional)

In order to get a better view of what Ray can mean for the customer, there is a possibility to opt for a **proof of concept (PoC)** before actually subscribing to Ray. For such a PoC, no private subaccount is created for customer. A temporary system is created in the Expertum subaccount and the customer's data is imported and analysed in the Expertum subaccount. The results with the own data will then be demoed to the customer.

During the proof of concept, the following steps will be executed:

- Download SAP Authorizations tables from the productive environment of the customer. This can be done in one of the following ways:
  - The customer provides the necessary files to Expertum, based on clear instructions and in a well-defined format.
  - Expertum gets (temporary) access to the productive environment of the customer and performs the downloads themselves.
  - The customer implements a download ABAP program provided by Expertum on their productive environment and perform the downloads by executing the ABAP program.
- Configure and prepare Ray for running analysis for the customer and perform a dashboard run on user level. This means uploading the downloaded productive data, running the risk analysis with a default ruleset (see further) and displaying the results in the dashboards of the app.
- Export the results to Excel as deliverable for the customer.
- Present the dashboards with the own data.

The PoC run will be performed using a default Expertum ruleset. This means:

- No completeness of all potential risks will be achieved;
- No own developed transaction codes will be considered, nor will there be any custom authorization objects or customer specific authorization values (like own movement types, document types, etc.) taken into account.
- The Expertum ruleset used is the one we use during our Health Check service. This ruleset contains the following:
  - 116 Critical Access Risks.
  - 148 SOD Risks.
  - 1 Critical Permission Risk

The **proof of concept** of **Ray** is offered at a fixed fee. If the customer opts for such a PoC, a separate, preliminary workorder will be made for this.

If after finalizing the PoC the customer would subscribe to Ray, a 1-time discount will be granted on the app subscription price. This 1-time discount will be applied on the first workorder for the licenses. This discount will only apply when:

- The subscription was done within 3 months after performing the PoC.
- The subscription is taken for a minimum of 1 year.

6 Authorizations Health Check (Optional)

The risk results and the usefulness of Ray heavily depend on the implemented authorizations concept. The authorizations concept forms the basis for the overall control level of your authorizations. In case you are not sure about the quality of your current authorizations setup, Expertum's **Authorizations Health Check** will validate if the authorization structure is maintained in line with best practices, maintenance efficiency and risk considerations. The customer can opt for having such an Authorizations Health Check performed before actually subscribing to Ray.

The following steps are executed during the analysis:

- Download SAP Authorizations tables from the productive environment of the customer. This can be done in one of the following ways:
  - The customer provides the necessary files to Expertum, based on clear instructions and in a well-defined format.
  - Expertum gets (temporary) access to the productive environment of the customer and performs the downloads themselves.
  - The customer implements a download ABAP program provided by Expertum on their productive environment and perform the downloads by executing the ABAP program.
- Prepare the Expertum analysis tools for the Health Check.
- Technical review / quality check of the authorization role set-up.
- Analysis of SOD issues in single, derived and composite roles. This is also performed by Ray.

The following deliverables are foreseen:

- A Powerpoint review report of the current authorization role set-up
- A Segregation of Duties analysis of the single roles, derived roles and composite roles, assessed against the "Expertum standard SOD Ruleset"
- Recommendations for improvements
- A workshop to discuss the outcome of the Health Check and possible next steps

The **SAP Authorizations Health Check** is offered at a fixed fee. In case, however, this Health Check is performed in combination with a Proof of Concept, then the fixed fee will be reduced.

If the customer opts for an Authorizations Health Check, a separate, preliminary workorder will be made for this.

7 Appendices

7.1 Appendix 1: SAP GTC for Cloud Services

7.2 Appendix 2: Expertum Terms & Conditions