Engagement Guidance

Getting Started with the SAM GDPR Assessment

The SAM GDPR Assessment helps customers create a better understanding of their existing practices in relation to the General Data Protection Regulation (GDPR). This document is a companion to the SAM GDPR Engagement Toolkit and guides the execution and creation of the customer assessment and report.

Topics in this document include:

<table>
<thead>
<tr>
<th>Introduction to the GDPR (EU) 2016/679</th>
<th>Organizational Topics GDPR Basics</th>
</tr>
</thead>
<tbody>
<tr>
<td>The introduction to the EU data protection law</td>
<td>Organizational aspects of governance, risk, practices, review, and management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technical Topics CIS v7 Controls</th>
<th>Report Building</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical controls selected based on their association with the regulation and level of criticality</td>
<td>A practical guide to report creation based on the example report provided in the toolkit</td>
</tr>
</tbody>
</table>
Contents

Introduction ........................................................................................................................................... 3
  GDPR Introduction .............................................................................................................................. 3
Engagement Background ......................................................................................................................... 4
GDPR Basics ........................................................................................................................................ 5
  Fundamentals ...................................................................................................................................... 5
  Definitions .......................................................................................................................................... 5
  Data Subject Rights ............................................................................................................................ 7
  Organizational Responsibilities ........................................................................................................... 8
  Additional Information ....................................................................................................................... 11
  References .......................................................................................................................................... 11
CIS Controls Framework ....................................................................................................................... 12
  CIS V7 Controls Structure .................................................................................................................. 12
  CIS V7 Controls Questionnaire .......................................................................................................... 12
SAM GDPR Engagement Deliverable Guidance .................................................................................. 13
  Assessment Goals ............................................................................................................................. 14
  Example Report Structure .................................................................................................................. 14
  Measurement Considerations ............................................................................................................ 16
  Findings and Recommendations ........................................................................................................ 16
Introduction

This document is a companion to the SAM GDPR Engagement Toolkit, providing guidance for the SAM GDPR Assessment and development of the SAM GDPR Assessment Report. A measurement scheme utilizing the Microsoft Security Maturity Model (v1) provides the Organizational and Technical topics to report on customers’ practices related to the General Data Protection Regulation (GDPR).

To provide a measurable set of technical controls aside from those required by GDPR, the assessment utilizes the CIS v7 Controls™ framework published by the Center for Internet Security®. A selection of controls referring to the articles of the GDPR was taken from the CIS v7 Controls framework providing a baseline for data protection practices.

This guidance document and the checklist provided in the SAM GDPR Questionnaire is designed to help SAM Partners execute the assessment and use the Questionnaire and the example SAM GDPR Assessment Report referenced in this document to create a deliverable that is consistent with the goals of the Microsoft SAM GDPR Engagement Statement of Work (SOW).

GDPR Introduction

In 1995 the (Data Protection) Directive 95/46/EC went into effect in the European Union (EU), a point in time during which the common thinking about the concept of privacy was mostly related to physical privacy. Privacy was not a common concern, beyond physical situations like protecting a personal information from onlookers during ATM use, for example. Personal information was only digitalized by governmental agencies, companies, and organizations in order to facilitate administrative processes. Personal data was not considered a valuable asset.

Digital privacy wasn’t a public concern at that time, when the internet was just emerging. Personal information was provided to (web)shops, healthcare institutes, and any other commercial organization without question or consideration for the relevance or consequences. In those days, consumers were unknowingly increasing the commercial value of their personal data by sharing it. Nobody could have imagined technology would transform life at such a fast pace, and in less than two decades nearly every world citizen would come to have an extensive digital footprint.

As the Data Protection Directive was not binding and only provided guiding principles for the EU Member States, the transformation to a digital lifestyle demanded harmonization of the laws within the EU on the protection of personal data. In 2012 a proposal initiated the comprehensive reform of Directive 95/46/EC in order to increase the digital privacy rights of individuals. After nearly 4 years, the GDPR Regulation 2016/679 entered into force on May 24th, 2016. Member States were given 2 years to implement and, enforce the law by May 25th, 2018. At the time of writing this document, the regulation applies to any governmental agency, public service, company, and organization, regulating the right to privacy through data protection in the European Union.

‘Privacy – a fundamental right’
Engagement Background

The SAM GDPR Engagement was designed to provide value to Microsoft customers beyond a basic SAM engagement, which focuses on the deployment and usage state of Microsoft products and license entitlement. The GDPR assessment focuses on the effectiveness of the customer’s current GDPR practice from an organizational and technical perspective compared to a baseline of requirements.

Any organization, in- or outside the European Union, collecting or processing personal data of individuals within the perimeters of the Europe Union must take action to comply with the requirements of the GDPR.

With the introduction of the GDPR, the traditional mindset towards privacy and data protection is no longer satisfactory. Privacy and data protection are bound together, which requires organizational change. The GDPR requires that organizations respect the rights of individuals and prove accountability through responsible data protection.

This assessment measures the impacts of that shift at both organizational and technical levels, as shown here by comparing traditional environments with privacy-aware environments.

<table>
<thead>
<tr>
<th>Traditional Environments</th>
<th>Privacy-Aware Environments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business-/commercial-centric strategy</td>
<td>Privacy-centric strategy</td>
</tr>
<tr>
<td>Common security awareness</td>
<td>Organization-wide security and privacy culture</td>
</tr>
<tr>
<td>Ad-hoc business with partners/suppliers</td>
<td>Pre-arranged (processing) agreements</td>
</tr>
<tr>
<td>Focus on the business applications as assets</td>
<td>Focus on data as a company asset</td>
</tr>
<tr>
<td>Security group based, individually defined access</td>
<td>Business role-based access with justifiable proof on access with checks/audits</td>
</tr>
<tr>
<td>Security practice to protect IT assets</td>
<td>Security practice to protect data subject privacy</td>
</tr>
</tbody>
</table>

During the GDPR assessment, the SAM Partner collects information using the checklist provided in the SAM GDPR Questionnaire outlining the organizational and technical practice position of the customer. In addition to the manual or automated technical scans on all Microsoft product deployments, usage, and versions, the SAM Partner will use third-party tools and have interviews with key customer stakeholders, to capture all information and data relevant to the assessment as outlined in the Statement of Work.

The definitions in this guide are key to gaining an understanding of the GDPR fundamentals. With this understanding, the information and data collected, the Partner provides an analysis of the findings as well as recommendations using the SAM GDPR Assessment Report.

**This assessment in no way guarantees compliance with the GDPR, but instead provides a foundation for understanding the data environment, processes, and capabilities as they relate to the GDPR, privacy, and data protection.** In no event will the SAM Partner make any statement to a customer that this SAM GDPR Assessment will bring them into compliance with the GDPR regulation.
GDPR Basics

Fundamentals

The GDPR does not provide a set of measures or controls, but instead is founded on 173 recitals which justify the 99 articles of the GDPR. The regulation provides a combination of high-level legal, organizational, and technical requirements. It is important to remember that the regulation does not regulate privacy. It regulates data protection, which protects individual privacy.

The principles relating to ‘processing’ of ‘personal data’ bound to ‘rules’ for organizations and ‘rights’ of individuals are the foundation of the regulation. The rights of a ‘data subject’ (natural person) and regulatory rules that apply to a ‘controller’ (natural or legal person, public authority, agency, or other body) being responsible, are in the essence of the regulation.

Severe penalties and fines can be imposed for violating the GDPR. Administrative fines of up to € 20 million or 4% of annual turnover in the previous financial year may be levied. In addition, penalties such as seizure of profits or permanent prohibition of processing personal data could also be imposed. Although the GDPR is restrictive, it does, however, open opportunities for organizational and technological innovation and use of the latest cloud technologies.

Definitions

To gain a proper understanding of the contents of the regulation and to be able to provide to correct answers to the Questionnaire it is of utmost importance to understand the official definitions. As this engagement focusses on a baseline assessment, only a few definitions will be explained in more detail.

- ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
  
  o Explanation: information that could potentially lead to the identity of a person. For example, a name, address, birthdate, email address, IP address or a picture either by itself or combined.

Important Notes:

- (1) The regulation defines ‘special categories of personal data’. This is information related to: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation and shall be prohibited. For this reason, a picture/photo, reveals a person’s racial or ethnic background, and possibly other characteristics, and is considered as information of a special data category.

- (2) Two example scenarios in which data in a special category could still be allowed for processing is when the ‘data subject’ has given explicit consent or in case of requirements in the field of employment, social- security or protection laws. (See Article 9)
(3) Information related to **criminal convictions and offences** are only allowed for processing by official authorities.

- **‘processing’** means **any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction**;
  
  o Explanation: processing refers to any action on personal data, regardless of the form in which the personal data is stored. Modifying a document, making a backup, copying a database and log files containing personal data, or unpacking a compressed file.

- **‘controller’** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
  
  o Explanation: any governmental agency, public service, company, organization, or otherwise, that receives information about/from ‘data subjects’. A ‘controller’ is responsible and needs to demonstrate accountability.

- **‘processor’** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
  
  o Explanation: a processor only processes data following the exact instructions provided by the controller. This is typically an outsourced party, like a payroll company, which has been given ‘personal data’ from another organization in order to perform a predetermined contractual action. As soon as the ‘processor’ is able to determine the purposes and means of the personal data it receives, it becomes a ‘controller’ or ‘joint-controller’. An organization can be a “controller” and “processor” at the same time.

- **‘supervisory authority’** means an independent public authority which is established by a Member State pursuant to Article 51;
  
  o Explanation: the authority supervising the controller, processor or any other related subject to the regulation. Each country within the EU has assigned a local authority to provide advice on the regulation and to investigate any “incidents” related to data protection and violations to the rights of ‘data subjects’.
Data Subject Rights

Harmonization of fundamental individual rights and freedoms throughout the European Union, and particularly the protection of personal data, was essential to the European Commission in establishing the GDPR. Transparent information, communication, and methods for exercising individual rights are anchored in the regulation.

Organizations should be well aware of these rights as a request by a data subject (also employees of the organization) is time limited and must be answered, unless the data subject cannot be identified.

The Data Subject (natural person), in relation to their personal data, has the right to 'information' and 'access' to personal data, right of 'rectification' and 'erasure', 'restriction of processing', 'object', 'data portability' and 'object to automated processing'. These eight (8) rights are fundamental under the regulation and bind any organization.

1. **Right to be Informed**
   Individuals have the right to request information on which of their personal data is being processed and the related reasons and justifications for processing.

2. **Right of Access**
   This right allows individuals to request a copy of their personal data being processed.

3. **Right to Rectification**
   If an individual believes the information held is not up-to-date or accurate, a request for modification of the personal data can be made.

4. **Right to Erasure**
   Also called the “Right to be forgotten”, this right provides individuals the ability to request the removal of personal data. If an individual withdraws consent to processing the personal data, it is a legitimate reason to request the removal of personal data if there are no other legal grounds for processing.

5. **Right to Restrict**
   An individual has the right to restrict or deny (specific) processing of personal data.

6. **Right to Data Portability**
   Individuals have the right to request their personal data for processing by another 'controller', 'processor', or for personal purposes. This request may not be obstructed in any way.

7. **Right to Object**
   Under certain circumstances, individuals are entitled to object to the use of their personal data. This can be related to scientific, historical, or marketing purposes.

8. **Right to Object to Automated Processing**
   This right provides an individual with the ability to object to a decision based on automated processing and request human intervention in the decision making process. Automated processing also includes profiling based on the personal data of the individual.
Organizational Responsibilities

In the essence of the regulation, organizations are responsible for the protection of personal data and demonstrating accountability to the general public. The regulation contains a large number of rules which apply to all “controllers” and “processors”. Although the rules dictated by the regulation are mandatory and process driven, the regulation also demands a risk-based assessment to determine the necessity for more restrictive regulatory and technical measures on processing personal data.

The key regulatory processes and measures will be discussed in this chapter in order to provide a better understanding for the SAM Partner on the organizational topics in the SAM GDPR Questionnaire.

1. Governance
   - **Privacy Policy**
     As with all organizational policies, the privacy policy reflects the organization’s position on the subject of privacy. The privacy policy should describe the ways “personal data” is collected, used, disclosed, managed, and secured. The privacy policy is a legal requirement and should establish transparency and accountability.

   - **Accountability**
     To demonstrate the organization’s transparency and proof accountability, it is important to explain in a clear way, for which purposes the organization uses “personal data” and therewith provide understandable justification. The division of tasks, responsibilities, and authorizations documented and established throughout the organization is meant to create organizational and individual accountability towards processing “personal data”.

     Disclosing the privacy policy through the means of a public statement demonstrates how serious an organization takes its accountability towards the general public. The statement should include a summary of the reasons and justification for collection, processing, and sharing. In addition, it should provide individuals with guidance on how to make a request to exercise their rights, including contact details (preferably of the Data Protection Officer). Complete transparency could be shown by disclosing the (summarized) “Record(s) of Processing Activities” providing direct insight on the actual data collected.

   - **Data Protection Officer (DPO)**
     The data protection officer focuses on the execution of the transparency and accountability in an independent oversight role. The DPO should identify, protect, and detect the issues and risks related to processing “personal data”.

     The GDPR requires the appointment of a DPO if the organization is a “public authority or body” or the core activities of the organization require “personal data” collection and processing on a regular basis and large scale. This also applies to systematic monitoring and profiling. As “large scale” is not defined in the GDPR, the thumb rule is that the assignment of a DPO is required for organizations that have 250 or more employees and/or data of 5000 or more data subjects is being processed.

     **Important Note:**
(1) The assignment of a DPO is mandatory if “special categories of personal data” are processed.

2. **Personal Data Handling**
   - **Records of Processing Activities**
     Data governance documented in “records of processing activities” is required to document the processing activities and related personal data. For the “controller”, an exhaustive record should exist and at least contain;
     
     a) the name and contact details of the controller and, where applicable, the joint controller, the controller’s representative, and the data protection officer;
     
     b) the purposes of the processing;
     
     c) a description of the categories of data subjects and of the categories of personal data;
     
     d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
     
     e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
     
     f) where possible, the envisaged time limits for erasure of the different categories of data;
     
     g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

   For a “processor” an exhaustive record should exist and contain;
     
     a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller’s or the processor’s representative, and the data protection officer;
     
     b) the categories of processing carried out on behalf of each controller;
     
     c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
     
     d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

**Important Notes:**

(1) The exceptions to the requirement of keeping records of processing activities are limited and commonly only apply to organizations that process “personal data” coincidentally or under unforeseen circumstances.

(2) By following the above list of requirements, the SAM Partner can reference the data locations from the samples or automated inventory taken from the customer.

(3) The “supervisory authority” may request the “records of processing activities”.

(4) The records must be digital, for example an Excel spreadsheet.
(5) Information related to employees is also considered “personal data”.

- **Data Processing Purpose Binding**
  Before collecting (and processing), the organization needs to determine and document the purposes and justifications for all processing of “personal data”. Unobvious reasons should be avoided in any case, and therefore clear, short and straightforward language is required. The purposes and justifications representing the use cases need to be documented in the “records of processing activities” of the “controller”.

- **Securing the Processing**
  This is a high-over topic for the organizational and technical measures to be taken. The organization shall ensure a level of security appropriate to the risks related to the processing activities. The Organizational and Technical topics in the assessment reflect a basic practice level on data protection. Article 32 of the GDPR outlines the requirements.

- **Transfer**
  If the organization has outsourced certain processing activities to a “processor”, the organization remains responsible for the “personal data” and therefore accountable for the actions of the “processor”. A processing agreement between the “controller” and “processor” should outline the mutual responsibilities in accordance to the GDPR. Confidentiality, integrity, availability and resilience should be topics covered in the processing agreement. Legal advice is demanded to ensure the completeness and lawfulness of such a contract between parties.

3. **Data Subject Rights Management**
   - **Quality Management**
     Monitoring the quality and accuracy while processing “personal data” is demanded to ensure the alignment with the statements in the “records of processing activities” and to be able to properly and accurately respond to a request by a “data subject”. Implementing a process and related procedures is required to provide continuous quality management.

   - **Access**
     An established process and procedure should be embedded in the organizational practices in order to provide “data subjects” access to their “personal data” on request. Accuracy, quality, and a proper understanding is demanded.

   - **Consent**
     A clear notice of data collection should be provided and appropriate consent for processing “personal data” should be obtained from a “data subject” prior to collecting or processing. Keeping records of the consents and related purposes is essential.

4. **Risk Management**
   - **Privacy by Design / Default**
     The enforcement of the strictest possible measures and privacy settings (organizational and technical) during the design of processing activities should be applied by default. The measures and settings should be maintained during the operational execution of the processing activities throughout the organization.
5. **Data Privacy Practices**
   - **Data Retention**
     Data retention and deletion policies should be defined and established for all "personal data" maintained and processed. The retention period should be recorded in the "records of processing activities" at the categories level. Deletion of data after the lawful justified retention period is mandatory.

6. **Review Data Privacy Practices**
   - **Evaluation and Monitoring**
     Continuous evaluation and monitoring of all practices related to processing of "personal data" including the review of policies, processes, procedures and measures is demanded to ensure data protection. At scheduled intervals the Data Protection Officer should initiate the reviews on the records of processing activities, processing agreements etc.

7. **Data Privacy Breach Management**
   - **Data Leaks**
     The local supervisory authority should be notified of "personal data" breaches in a timely fashion (72 hours). The data subject should also be informed of a data beach, unless an exception applies. Documentation of the breach as well as forensic investigation is required.

**Additional Information**

- Although not part of the SAM GDPR Assessment, "personal data" on paper and paper archives are also subject to the GDPR and should be under the attention of the customer.
- The local regulatory execution, enforcement, and requirements might differ between EU Member States and are not considered in the assessment. It is important for the customer to seek legal advice for full insights on EU Member State differences.

**References**

The official regulation and definitions (Article 4) can be found at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679) This is the official website of the European Union and also contains the regulation translated in 23 alternative languages.
CIS Controls Framework

The CIS Controls framework is a well-known and highly regarded security framework. The CIS Controls framework takes a community-based (as opposed to specific enterprise-based) approach to the notion of risk assessment. Instead of starting from the viewpoint of a specific enterprise (e.g., an agency or a facility), the CIS Controls were created using a consensus risk assessment process. This consensus risk assessment integrates the judgment of a large group of experts from government, industry, and academia regarding the common and pervasive threats and vulnerabilities that are typically found in large enterprises.

Since the CIS Controls were derived from the most common attack patterns and vetted across a very broad community of governments and industries, with very strong consensus on the resulting set of controls, it serves as a very strong basis for high-value actions. The framework does not attempt to replace comprehensive IT and security risk management frameworks. The CIS Controls, instead, provide focus and priority to a smaller number of actionable controls with high-leverage and high-payoff.

The technical topics assessed during the SAM GDPR Assessment are selected from the CIS V7 controls, which are the latest available. The selection of twelve (12) CIS V7 controls is made based on their connection to the terminology used in Article 32 of the GDPR and others. These focus on confidentiality, integrity, availability, resilience, and recoverability.

CIS V7 Controls Structure

The CIS V7 Controls are composed of three parts: Basic, Foundational, and Organizational. The first six (6) controls are considered the (Basic) foundation on security practices. Controls seven (7) through sixteen (16) are the Foundational controls and leverage common practices on security. The Organizational controls seventeen (17) through twenty (20) are focused on the organizational embedding of cyclic or continuous processes and the organization’s employees.

The CIS V7 sub-controls are labelled by Security Functions that can be described as follows:

- **Identify** – Discovery and inventory of the organization’s infrastructure, systems, assets, data, and capabilities.
- **Protect** – Implement the applicable activities, tools and measures to ensure a proper security practice.
- **Detect** – Implement the applicable activities, tools and measures to (be able to) identify the occurrence of a security event.
- **Respond** – Implement the applicable activities, tools, and measures to take action regarding a detected security event.

CIS V7 Controls Questionnaire

The CIS Controls are explained in detail in the SAM GDPR Questionnaire (Technical (CISv7)) tab. The questions for each of the twelve (12) selected controls are straightforward in terminology and language. In order to provide metrics on the selected CIS controls for the purpose of report building, the example report provides presentation examples.
A detailed description of the CIS v7 Controls can be found at: https://www.cisecurity.org/controls/

**SAM GDPR Engagement Deliverable Guidance**

A SAM GDPR Assessment Report is not meant to be a detailed control review or security audit. It is intended to provide an overall review of the programmatic aspects of an organization’s privacy and security program in an all-up approach, to determine whether it is aware of the risks revealed by, and the benefits of a privacy and security program given in line with the threats it faces and its overall IT risk appetite. Some organizations and industries are more risk averse or regulation-bound than others.

To achieve this goal, the SAM GDPR Assessment utilizes a maturity model to communicate findings and recommendations. The maturity model construct for the SAM GDPR assessment is based on a similar model developed by Microsoft (Security Maturity Model v1) and is consistent with the Software Optimization Model (SOM). The below reflects the levels:

<table>
<thead>
<tr>
<th>Basic (1)</th>
<th>Standardized (2)</th>
<th>Rationalized (3)</th>
<th>Dynamic (4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The program is tactical at best and the risks of a privacy issue are severe.</td>
<td>The program is proactive and the risks of a privacy issue are significant.</td>
<td>The program is holistic and fully operational and the risks of a privacy issue are moderate.</td>
<td>The program is strategic and optimal and the risks of a privacy issue are minor.</td>
</tr>
</tbody>
</table>

The levels reflect to the level of implementation represented in the organizational and technical context of a SAM GDPR Assessment. The assessment, analysis, and formulation of the recommendations may be either beyond the internal capabilities of SAM Partners or beyond the ability of SAM Partners to acquire that capability through a partner-to-partner (P2P) arrangement.

That said, the legal aspects of the assessment are a reasonable preliminary and valuable step to focus on a more in-depth subsequent assessment by a (GDPR) legal advisor or consultant who has the scope of practice to assess the implementation status through the definitions above.

The organizational and technical topics in the assessment embedded into the SAM GDPR Questionnaire have been developed to provide a reference for SAM Partners to deliver value to the customer as part of a SAM GDPR Engagement.

The checklist provided in the SAM GDPR Questionnaire will assist SAM Partners to complete the assessment and assure all information and data required is collected while the SAM Partner is on-site. The checklist allows the Partner to record the status of the assessment and provide a green-light upon completion of the assessment.
Assessment Goals

A SAM GDPR Assessment will provide a high-level review regarding the practices of an organization’s privacy and security program. The goals of the SAM GDPR Assessment are to:

- Provide transparency on the GDPR position of the customer to its management.
- Drive a change mindset towards GDPR compliance and organizational accountability.
- Initiate a foundation for the execution of Data Subject Rights.
- Align with the security “best practices” of a well-known and highly regarded security-framework as the foundation for data protection practices.
- Provide recommendations based on the interviews and from the facts found during the scan of the IT environment.
- Uncover critical issues related to cybersecurity.
- Establish a prioritized action list, based on the criticality of the findings which can serve as a short-term roadmap in the privacy journey of the organization.

Example Report Structure

The assessment criteria for the completion of the SAM GDPR Assessment Report are embedded in the SAM GDPR Questionnaire, through the checklist provided. The Questionnaire is specifically developed for the purpose of this assessment and only applies to the boundaries of the SAM GDPR Engagement. The suggested SAM GDPR Assessment report structure to present the findings, analyses, and recommendations is as follows:

- **Assessment Introduction**
  A standardized introduction providing background information on the GDPR, the assessment and high-level deliverables. Do not modify this section except for the customer’s name.

- **Scope of the Assessment**
  A section that captures the scope of the assessment based on information related to the customer and the SAM Partner. It includes a summary of the customer’s business objectives, core business applications, and IT landscape. This section requires customization per customer.

- **SAM GDPR Assessment Goals**
  An introduction to the approach used for the assessment, the Critical Security Controls framework, and the use of a maturity model construct. This section does not require customization of the example report except for the customer’s name.

- **Summary of Inventory Tools**
  A listing of the tools used to capture infrastructure data, typically the Microsoft Assessment and Planning (MAP) toolkit, but should also list other sources of inventory data such as Microsoft System Center or third-party discovery tools. This section requires customization per customer.
• **GDPR Summary**
  Explanation of the methods used for reporting and the first section containing actual results of the assessment. This section of the report requires customization per customer.

• **Company Rating**
  This section communicates a high-level view on the core topics and their rating. This section of the report requires customization per customer.

• **Organizational Recommendation**
  The example report is written in a way that this section requires modification when the report is delivered to different customers. This is the management abstract section, briefly outlining the essential risk factors. The length can be increased based on the customer’s situation and the SAM Partner’s expertise in privacy and security.

• **Organizational Topics**
  This section reflects the outcome of the questionnaire Organizational (GDPR) tab including the results, analyses, findings, and recommendations of the other inventories and data scan. This section of the report requires customization per customer.

• **Technical Topics**
  This section reflects the outcome of the questionnaire Technical (CISv7) tab including the results, analyses, findings, and recommendations of the other inventories and scans. This section of the report requires customization per customer.

• **Inventory Data**
  A fact-based reflection of the inventory data. This section of the report requires customization per customer.

• **Short-Term Roadmap**
  A summary of the most critical topics, arranged by organizational and technical aspects. This should reflect a usable one-page roadmap for the customer to be able to take immediate action on the mitigation of their risks related to privacy and security.

• **Addendum: Optional CIS v7 Controls**
  In case the Partner has additional findings that fit within the boundaries of the CIS v7 Controls framework, they can be reported in this addendum.
Measurement Considerations

For the measurement, consider the following simple terms for the levels:

- **Basic (1)**
  The customer does not meet the minimum requirements.

- **Standardized (2)**
  The customer meets the baseline and has just started to meet the requirements.

- **Rationalized (3)**
  The customer has implemented the requirements properly.

- **Dynamic (4)** - The customer has implemented the requirements completely and continuously improves and monitors them.

Findings and Recommendations

For the organizational and technical topics, the findings and recommendations section communicates the results of the questionnaire and technical scans and recommendations by the SAM Partner.

Many customers will find themselves in the Basic overall position but should be, at a minimum, at the Standardized level given the mandatory nature of the GDPR regulation and today’s threat landscape. Providing a proper explanation and clear understanding of the recommendations provided by the SAM Partner are therefore essential to add value for the customer.

The example report includes suggested wording for the findings and recommendations for the customer’s journey from Basic to Standardized as their future practice level.