Crayon | The Software Experts

Supporting your journey to GDPR compliance through SAM

Vicky Makhija
Director Consulting APAC

11 July, 2018

EU General Data Protection Regulation

The **General Data Protection Regulation (GDPR)** imposes new rules on organizations in the European Union (EU) and those that offer goods and services to people in the EU, or that collect and analyze data tied to EU residents, no matter where they are located.

→ **Enhanced** personal privacy rights

→ **Increased** duty to protect data

→ **Mandatory** breach reporting

→ **Significant** penalties for non-compliance

The Software Experts
Crayon

What are the key changes to address the GDPR?

Personal privacy

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

Controls and notifications

Organizations will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing

Transparent policies

Organizations must:

- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

IT and training

Organizations will need to:

- Train privacy personnel & employees
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create & manage compliant vendor contracts

Crayon
The Software Experts

Relationship between DPA and GDPR

PERSONAL DATA

The GDPR broadens the DPA's scope of personal data by including more detailed personal identifiers

MANUAL FILING SYSTEMS

The GDPR applies to BOTH automated personal data and to manual filing systems where personal data are accessible according to specific criteria

ACCOUNTABILITY

The GDPR introduces an accountability principle which requires organizations to demonstrate compliance through a series of actions and to maintain (easy-to-read) documentation that evidences those actions

CONSENT

Consent under the GDPR MUST be unambiguous and requires some form of clear affirmative action from users. This consent must be verifiable. Where consent has already been obtained under the DPA, organizations will not be required to obtain fresh consent (only) if it meets GDPR standards

INDIVIDUAL RIGHTS

The GDPR strengthens the rights of individuals to personal data including the:

- Right to be informed (concise, clear and free);
- Right of access
- Right to erasure
- Right to restrict processing;
- Right to data
- portability
- Right to object; and
- Rights to automated decision making and profiling

The Software Experts
Crayon

GDPR Key Highlights

Transparency and consent

The usage of personal data needs to be **defined and transparently communicated** to the data subject and the **consent must be obtained** unambiguously before data collection and/ or usage.

Remediation

Penalties and fines could be as high **as €20,000,000** or **4% total worldwide annual turnover** (whichever is higher). Effected individuals and corporations have the right to receive financial compensation.

Breach notification

All effected individuals and corporations need to be notified within **72 hours of any data compromise**.

Right to erase or port

Individuals have rights to **erase, restriction of processing** and **port personal data**.

The Software Experts
Crayon

How Crayon Can Help?

Enable you and your organisation to:

- ✓ Understand how GDPR will impact your business
- ✓ Assess the current capability & maturity
- ✓ Develop a clear GDPR strategy
- ✓ Define a roadmap leading to GDPR compliance

This will help you to:

- ✓ Plan effectively for meeting the GDPR compliance deadline and beyond

The Software Experts
Crayon

GDPR Key Highlights

1

STRATEGY & ORGANISATION
Management perception and attention, competencies, delegation of roles and responsibilities, risk evaluation etc.

2

POLICIES
Policies, rules, guidance, conduct etc.

3

PROCESSES & DOCUMENTATION
Processes, corporate governance, documentation etc.

4

DATA WORKLOADS

Data flow overview
Placement of data
Outsourced data
Data sensitivity

5

SECURITY SYSTEMS

Control mechanisms
Privacy by design
Backup of personal data
Data portability

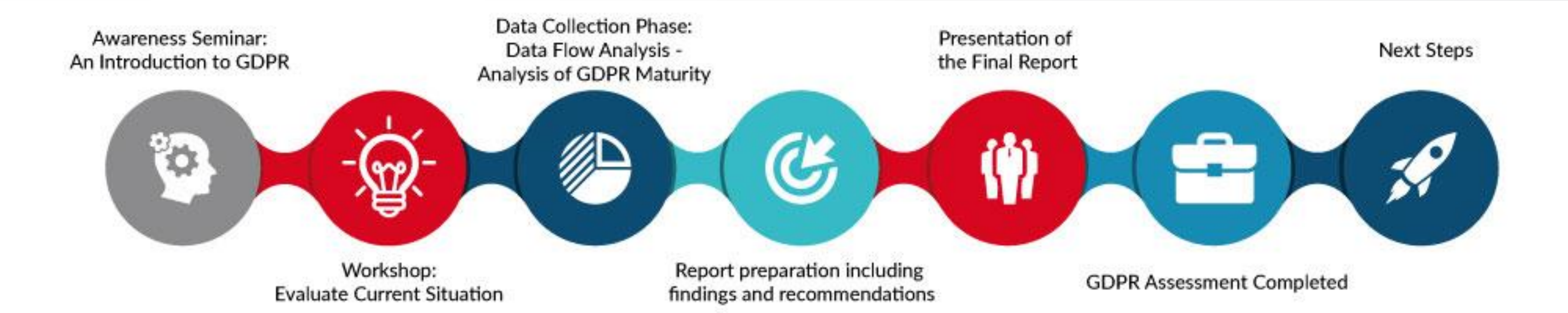
6

PHYSICAL SECURITY

Access control
Device security
Removable devices
Contracts, agreements, etc.

GDPR Assessment Phases

Data Collection, Workshop, Analysis and Delivery Phases



Awareness Seminar:
An Introduction to GDPR

Workshop:
Evaluate Current Situation

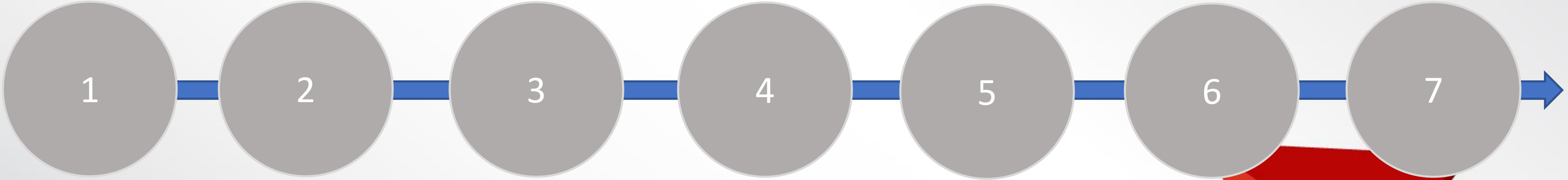
Data Collection Phase:
Data Flow Analysis -
Analysis of GDPR Maturity

Report preparation including findings and recommendations

Presentation of the Final Report

GDPR Assessment Completed

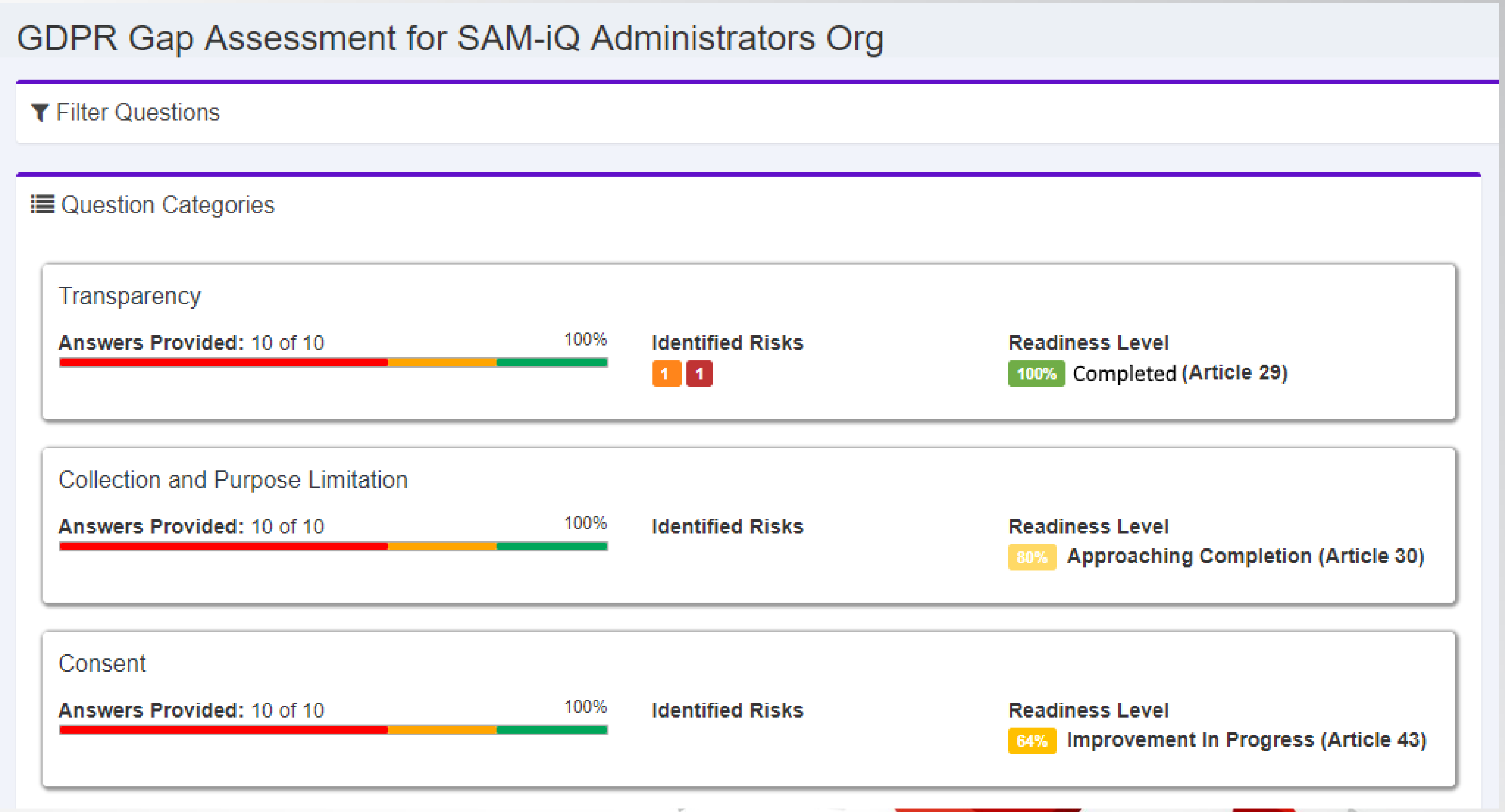
Next Steps



GDPR 360 Gap Analysis

✓ Online Gap Analysis

- Shows readiness level
- Identified risks
- Related to GDPR chapters, articles
- Detailed report identifying risks and action plan



GDPR Gap Assessment for SAM-iQ Administrators Org

Filter Questions

Question Categories

Transparency

Answers Provided: 10 of 10 100%

Identified Risks
1 1

Readiness Level
100% Completed (Article 29)

Collection and Purpose Limitation

Answers Provided: 10 of 10 100%

Identified Risks

Readiness Level
80% Approaching Completion (Article 30)

Consent

Answers Provided: 10 of 10 100%

Identified Risks

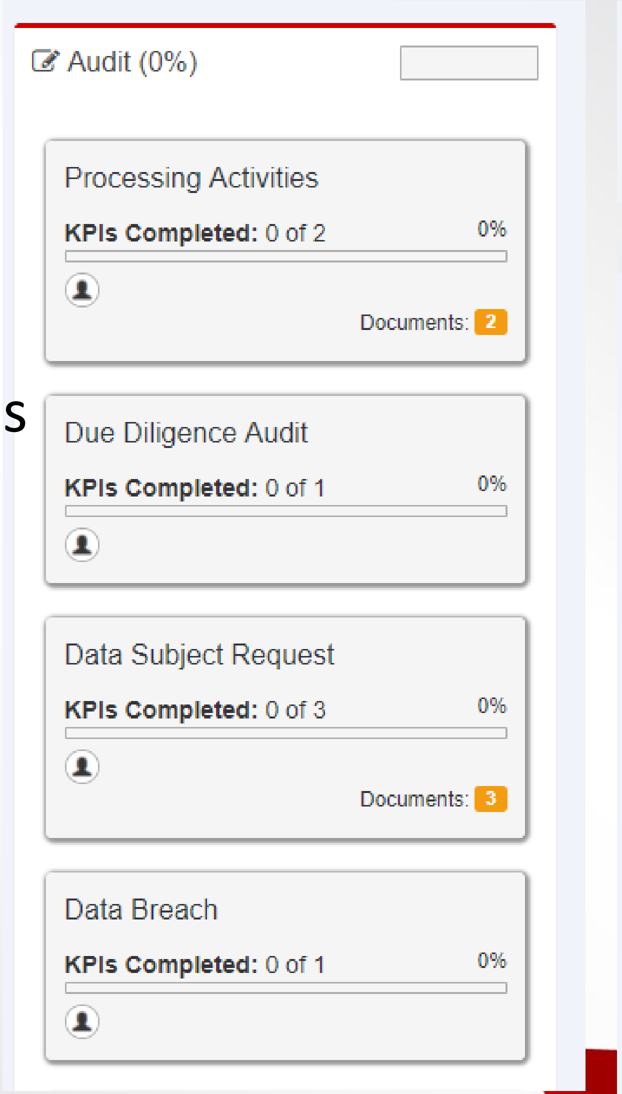
Readiness Level
64% Improvement In Progress (Article 43)

The Software Experts
Crayon

GDPR Readiness Tracker

Online Readiness Tracker Tool

- Objectives and KPI’s
- Related Article / Recitals associated to KPI’s
- Related Tasks and Documents



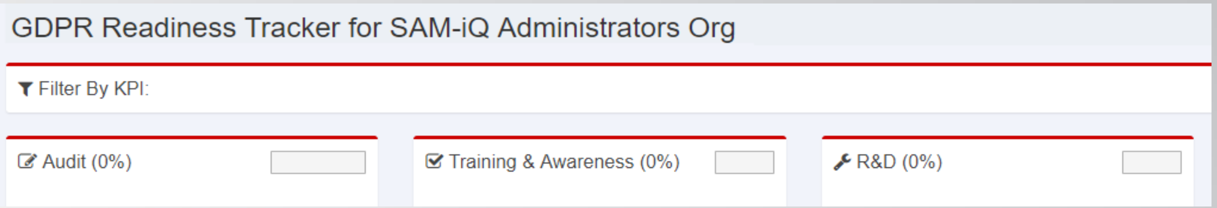
Audit (0%)

Processing Activities
KPIs Completed: 0 of 2 0%
Documents: 2

Due Diligence Audit
KPIs Completed: 0 of 1 0%

Data Subject Request
KPIs Completed: 0 of 3 0%
Documents: 3

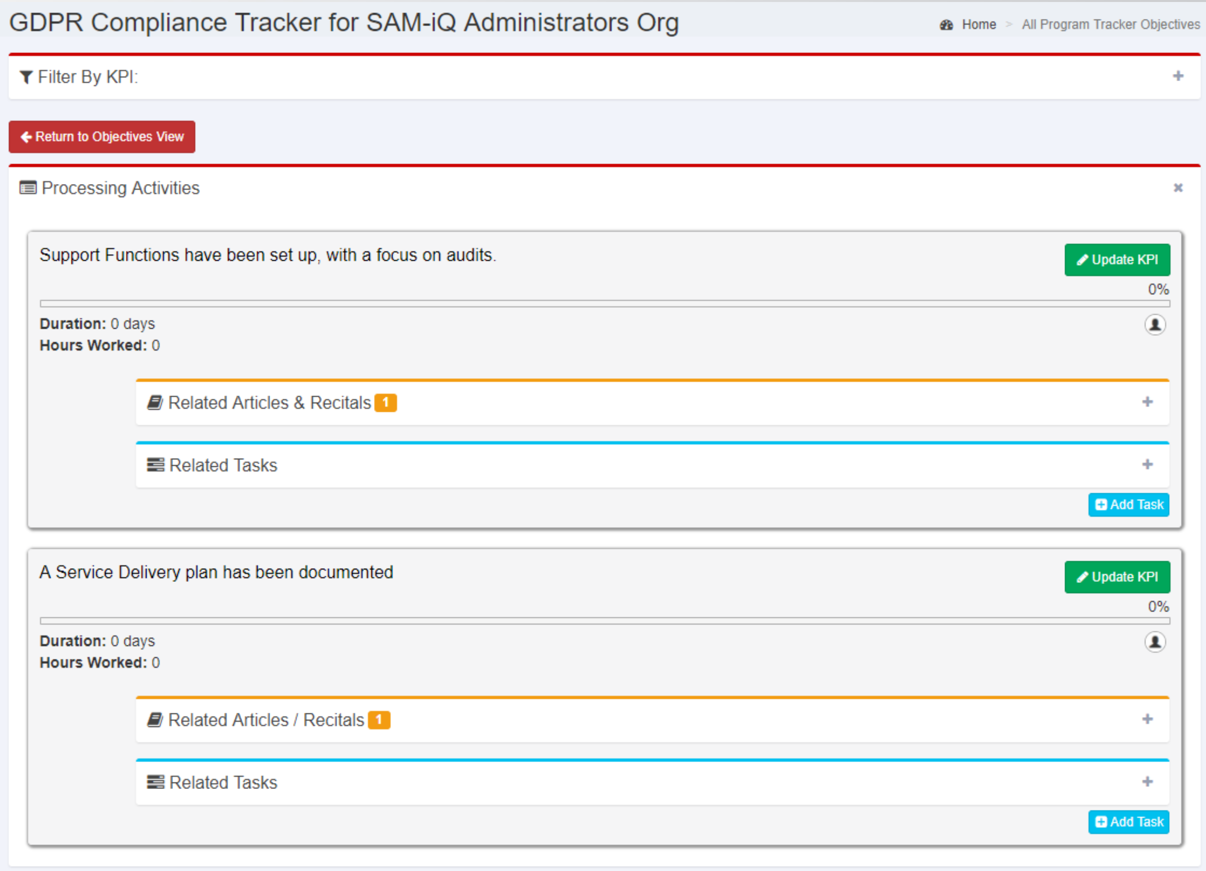
Data Breach
KPIs Completed: 0 of 1 0%



GDPR Readiness Tracker for SAM-iQ Administrators Org

Filter By KPI:

Audit (0%)
Training & Awareness (0%)
R&D (0%)



GDPR Compliance Tracker for SAM-iQ Administrators Org

Home > All Program Tracker Objectives

Filter By KPI:

Return to Objectives View

Processing Activities

Support Functions have been set up, with a focus on audits.

0%
Duration: 0 days
Hours Worked: 0
Related Articles & Recitals 1
Related Tasks

A Service Delivery plan has been documented

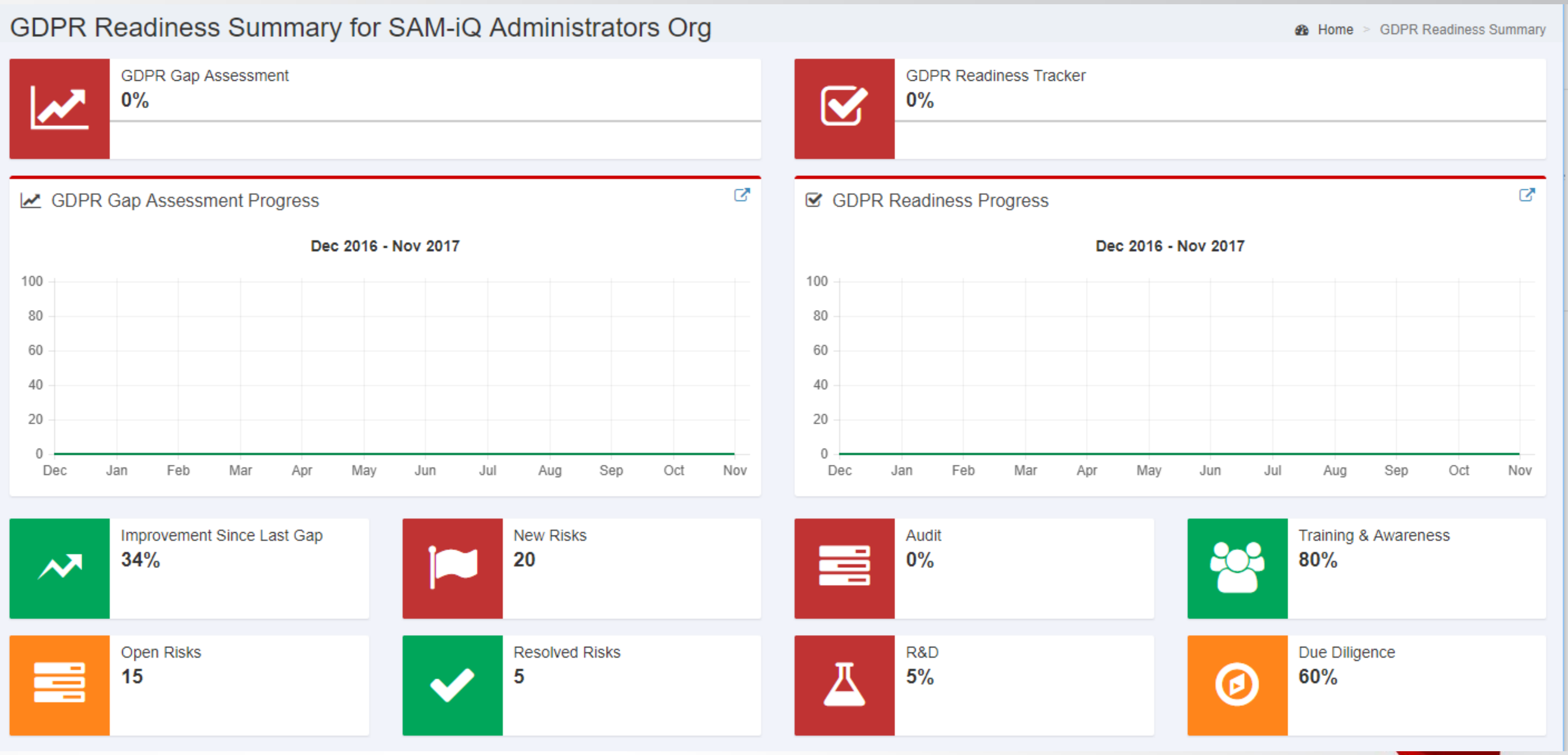
0%
Duration: 0 days
Hours Worked: 0
Related Articles / Recitals 1
Related Tasks

Crayon The Software Experts

GDPR Performance Dashboard

✓ Online GDPR Dashboard

- Gap % performance (point in time) with key statistics
- Current Readiness level % with breakdown by phase



GDPR Readiness Summary for SAM-iQ Administrators Org

Home > GDPR Readiness Summary

GDPR Gap Assessment
0%

GDPR Readiness Tracker
0%

GDPR Gap Assessment Progress

Dec 2016 - Nov 2017

GDPR Readiness Progress

Dec 2016 - Nov 2017

Improvement Since Last Gap
34%

New Risks
20

Audit
0%

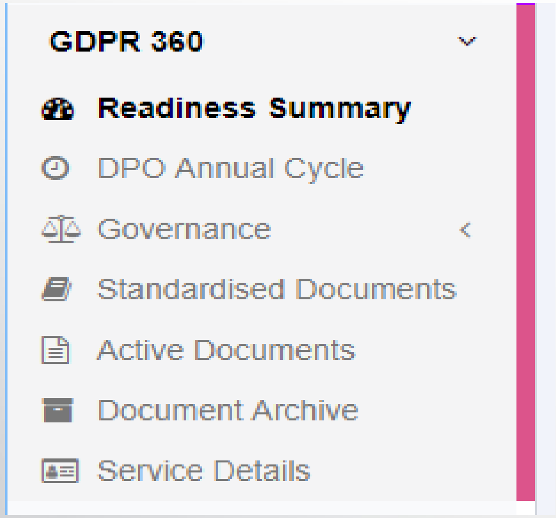
Training & Awareness
80%

Open Risks
15

Resolved Risks
5

R&D
5%

Due Diligence
60%

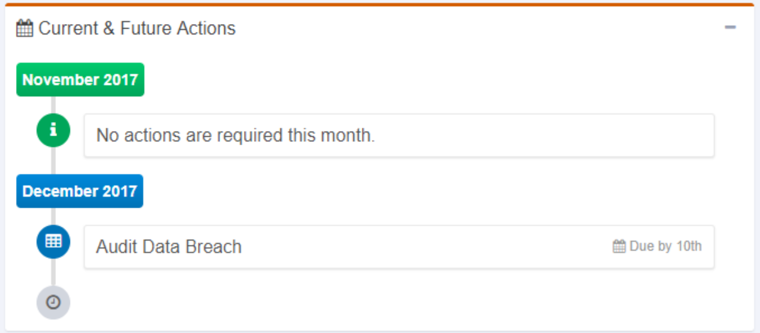


GDPR 360 DPO Annual Cycle

Crayon — The Software Experts

DPO tools:

- Mange actions
- Allocate resources
- Manage tasks
- Maintain



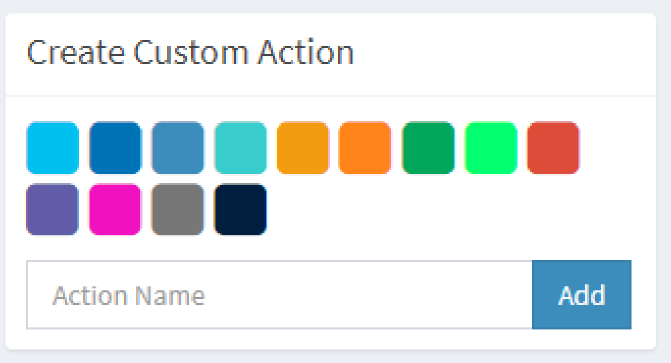
Current & Future Actions

November 2017

No actions are required this month.

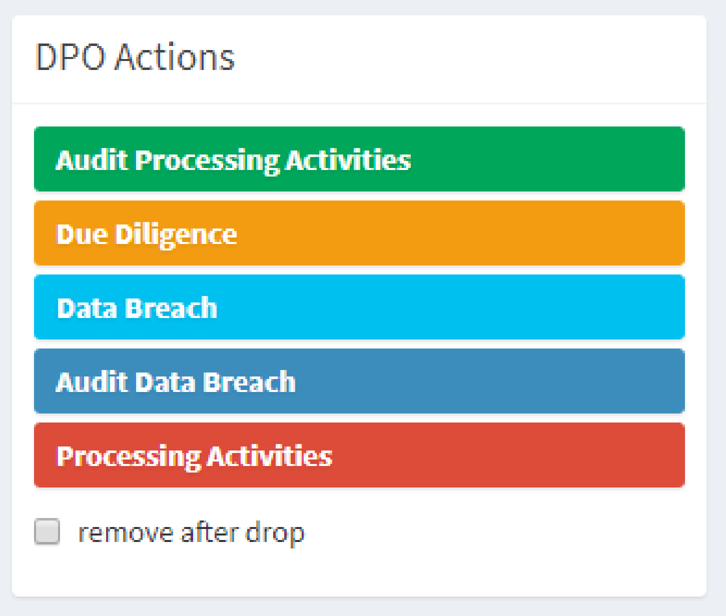
December 2017

Audit Data Breach — Due by 10th



Create Custom Action

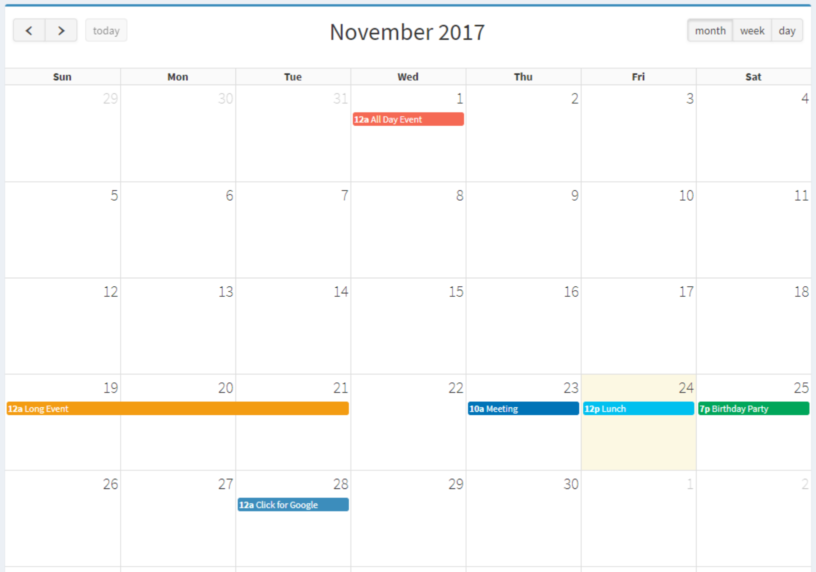
Action Name — Add



DPO Actions

- Audit Processing Activities
- Due Diligence
- Data Breach
- Audit Data Breach
- Processing Activities

☐ remove after drop



November 2017

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1 12a All Day Event	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19 12a Long Event	20	21	22	23 10a Meeting	24 12p Lunch	25 7p Birthday Party
26	27	28 12a Click for Google	29	30	1	2

© MARK ANDERSON
WWW.ANDERTOONS.COM
ANDERSON

“Before I write my name on the board, I’ll need to know how you’re planning to use that data.”

Contact

- @Vicky_Makhija
- vicky.makhija@crayon.com
- https://sg.linkedin.com/in/vickymakhija