Grant Thornton
An instinct for growth™

Sheffield City Region Mayoral Combined Authority and South Yorkshire Passenger Transport Executive

General Data Protection Regulation - Internal Audit

March 2020

Andrew Smith
Director
T: 0161 953 6900
E: andrew.j.smith@uk.gt.com

Lisa MacKenzie
Internal Audit Manager
T: 0121 232 5157
E: lisa.p.mackenzie@uk.gt.com

Robert Toogood
Subject Matter Expert / Cyber Consulting
T: 07768 251775
E: robert.j.toogood@uk.gt.com

Contents

Report distribution:

- Dave Smith, Managing Director (SCRMCA)
- Stephen Edwards, Executive Director (SYPTE)
- Steve Davenport, Principal Solicitor and Secretary (DPO) (Group)
- Ruth Adams, Deputy Managing Director (SCRMCA)
- Noel O'Neill, Interim Group Chief Financial Officer
- Stephen Batey, Head of Governance and Compliance (SCRMCA)
- Mike Thomas, Head of Financial Services
- Andy Dickinson - Head of Information Technology (SIRO) (SYPTE)
- Claire James, Senior Governance and Compliance Manager (SCRMCA)
- Christine Marriott - Scrutiny Officer (SCRMCA)
- Nick Brailsford, IT Operations Manager (SYPTE)
- Rachael Radford, Head of HR (SYPTE)
- Nigel Cairns, Head of Infrastructure (SYPTE)

For action

- Claire James, Senior Governance and Compliance Manager (SCRMCA)
- Andy Dickinson, Head of Information Technology (SIRO) (SYPTE)
- Stephen Batey, Head of Governance and Compliance (SCRMCA)
- Christine Marriott, Scrutiny Officer (SCRMCA)
- Nick Brailsford, IT Operations Manager (SYPTE)
- Rachael Radford, Head of HR (SYPTE)
- Nigel Cairns, Head of Infrastructure (SYPTE)

Responsible Executives:

- Steve Davenport - Principal Solicitor and Secretary (DPO) (Group)

It is the responsibility solely of the Sheffield City Region Mayoral Combined Authority and South Yorkshire Passenger Transport Executive management and directors to ensure there are adequate arrangements in place in relation to risk management, governance, control and value for money.

Grant Thornton | An instinct for growth™

Executive Summary

Objectives

We achieved our audit objectives by:

- Interviewing staff responsible for areas covered by the IASME Governance Self-Assessment Questionnaire analysis
- Performing a walkthrough of the Authority's processes to confirm our understanding
- Interviewing staff responsible for implementing GDPR projects as part of the remediation activities to understand from them:
  - Which projects exist
  - How projects are run
  - How progress is reported
- Reviewing documentation to align GDPR Action Plan remedial activities with IASME Governance Self-Assessment Questionnaire non-compliant areas
- Reviewing policies and procedures that evidence compliance with GDPR surfaced through analysis when spot checking answers
- Interviewing staff responsible for GDPR Action Plan activities to understand from them:
  - Are plans well understood with clear objectives
  - Have appropriate stakeholders been identified and engaged
  - Has sufficient resource, at the right level of experience been assigned
  - Has budget (where required) been assigned

The findings and conclusions from this review will feed into our annual opinion to the Audit Committee on the adequacy of the Authority's overall internal control environment.

Conclusion

Significant assurance with some improvement required

The main purpose of the audit was to assess overall compliance with the GDPR as it has been implemented in the UK ie the Data Protection Act 2018 (DPA2018), which became law in May 2018.

We have been able to find extensive evidence of good practice being used by dedicated, professional and very busy organisations. This reflects the sound work undertaken in initially meeting the GDPR/DPA2018 requirements, and subsequent activities to improve the effectiveness of what was originally implemented. However, whilst there are a few control related issues, there are also many opportunities which we have identified to extend further the initial work to create a more robust, comprehensive and efficient level of compliance with this challenging and wide-ranging legislation.

We have concluded that the processes provide a **SIGNIFICANT ASSURANCE WITH SOME IMPROVEMENT REQUIRED** level of assurance to the Board.

Our findings are subsequently summarised in the Action Plan section of this report.

Executive Summary

Good practice

- Comprehensive GDPR related management processes with supporting policies and procedures, although sometimes different in content and approach
- Comprehensive manual mapping of systems and processes using personal data across, using an Information Asset Register based approach although in some areas these registers are different and need updating
- Evidence of active and ongoing training and awareness activities
- Evidence of engaged leadership team, with clearly delegated powers to an effective and well managed group of officers
- Indirect evidence that the Authority is using a risk-based approach to GDPR in most areas although some areas of potential exposure haven't been fully addressed eg Third Party Supplier Management

Areas requiring improvement

- Third Party Supplier Management (low)
- Information Asset Management (low)
- Information Security Classifications (low)
- Risk Management (low)
- Website Accuracy (low)

Other improvement areas for consideration

- Controls Framework
- Quality Management Policies and Procedures
- Future Developments and Plans
- Compliance Management Automation
- Log File Management
- HR Platform
- Backup Data Protection
- Self Auditing
- Unstructured Data

Recommendations

The table below sets out the number and nature of recommendations set out in this report.

	High	Medium	Low	Improvement points
Recommendations	0	0	5	9

Acknowledgement

We would like to take this opportunity to thank your staff for their co-operation during this review.

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
1 (low)	Third Party Supplier Management Whilst there are legal, contractual clause in place to ensure suppliers are aware of what is expected of them, there are minimal due-diligence checks undertaken, on a risk-based approach to independently assess the security posture of third party suppliers.	**Key findings** The third-party payment provider and payroll service have not been independently assessed (due diligence) to ensure it is compliant with GDPR/DPA2018 legislation and documentary evidence secured to confirm this.		**Agreed Actions:** Agreed, on a case by case risk approach. **Responsible Officer:** Procurement Teams **Executive Lead:** Steve Davenport **Due Date:** 01/08/2020
		1	**Recommendation** Introduce a new due-diligence process across both organisations to ask suppliers handling GDPR/DPA2018 designated personal data to complete an initial information security assessment questionnaire, possibly based on the Cabinet Office's Supplier Assurance Framework: Good Practice Guide and then, depending on the risk level present, conduct further independent checks. See Key Recommendation Guidance on page 19 for more information.	

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
2 (low)	Information Asset Management Each organisation has a different Information Asset Register process, with different register formats and interpretations of what is needed, and missing entries relating not just to content but also scope.	**Key findings** Each organisation uses a different Information Asset Register (IAR) format. SYPTE's IAR only contains a small subset of the fields used by SCRMCA, and does not clearly identify the associated Security Classification and other details which should be tracked and actively managed/maintained. SCRMCA's IAR does not recognise that some of their data is being processed on their behalf by SYPTE's eg HR and Finance related data in SYPTE's HR WorldServices platform and SYPTE's Finance outsourced payroll service.		**Agreed Actions:** Agreed, to standardise information asset register. **Responsible Officer:** Claire James and Andy Dickinson **Executive Lead:** Andy Dickinson and Stephen Batey **Due Date:** 01/12/2020
		2	**Recommendation** Review the way in which the Information Asset Register is used across both organisations and look for an opportunity to standardise on a more consistent, comprehensive version that includes all key fields that should be tracked for both organisations in line with the requirements of GDPR/DPA2018.	

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

<table>
<tr><th>Rec #</th><th>Issue</th><th colspan="2">Findings and Recommendation</th><th>Action Plan</th></tr>
<tr><td rowspan="2">3

(low)</td><td rowspan="2"><u>Information Security Classifications</u>

Not all data/sources have had an appropriate information security classification assigned, particularly in the area of the significant amount of official-sensitive HR related data that resides in multiple locations across the two organisations systems in both structured and un-structured forms.</td><td colspan="2">Key findings

Data classification criteria should be reviewed as part of regular ongoing cycle of Data Audit in both organisations, and reflected in updates to IAR’s (ref back to Cabinet Office guidance on use of Official-Sensitive). SYPTE’s IAR only contains a small subset of the fields used by SCRMCA, and does not clearly identify the associated Security Classification which should be used.</td><td rowspan="2">Agreed Actions:

Agreed, review the way information security classifications are used across both organisations.

Responsible Officer:

Stephen Batey and Andy Dickinson

Executive Lead:

Steve Davenport

Due Date:

31/03/2020</td></tr>
<tr><td>3</td><td>Recommendation

Review the way in which the Information Security Classifications are being used across both organisations to support GDPR/DPA2018 compliance to ensure that they are being used consistently, in line with Cabinet Office guidance on Government Security Classifications, both from a classification and protection of data perspective.

See Key Recommendation Guidance on page 20 for more information.</td></tr>
</table>

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
4 (low)	Risk Management Separate systems are being used by both organisations, with cyber and GDPR related risks only being held and managed at a summarised level.	**Key findings** Different systems are being used in each organisation to manage risks; SYPTE uses 4Risk and SCRMCA uses spreadsheets. No detailed risk management procedure available for review, other than high-level policy. Risks eg Cyber and GDPR are being managed at a summarised level in both organisations.		**Agreed Actions:** Agreed, review how GDPR related risks are being managed across both organisations. Risk registers to be updated following review. **Responsible Officer:** Claire James and Andy Dickinson **Executive Lead:** Steve Davenport **Due Date:** 01/09/2020
		4	**Recommendation** Review the way GDPR/DPA2018 related risk is being managed across both organisations to look for ways of implementing a more consistent, lower level process which identifies and manages lower level risks and not higher level summary risk groupings.	

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
5 (low)	Website Accuracy Some key documents referred to on the websites of both organisations are out of date, including the IT Policy last updated in April 2011 and an incorrect reference on SCRMCA's Procedures page to the DPA1998.	**Key findings** SCRMCA's website incorrectly refers to the 1998 DPA on Procedures page. SCRMCA website on Procedures page links IT Policy back to SYPTE's but in this policy, last updated in 2011, there is no reference to SCRMCA and is out-of-date.		**Agreed Actions:** Agreed, the public facing websites will be updated, and a new IT Policy will be implemented in April 2020. **Responsible Officer:** Christine Marriott and Andy Dickinson **Executive Lead:** Andy Dickinson **Due Date:** 01/04/2020
		5	**Recommendation** Review cross-referencing of documents on all public-facing websites to ensure that references to GDPR/DPA2018 related legislation is correct and linked documents are updated to reflect the context in which they are being referred to.	

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
6 (imp)	<u>Controls Framework</u> No controls framework in place to help manage ongoing compliance with requirements of GDPR and other related compliance legislation.	**Key findings** There is no ongoing, proactive overall process for early detection and correction of control deficiencies before an audit.		**Agreed Actions:** Implement Cyber Essentials Plus in 2021 and review further requirements thereafter. **Responsible Officer:** Nick Brailsford **Executive Lead:** Andy Dickinson **Due Date:** 01/03/2021
		6	**Recommendation** Investigate the use of a suitable full or partial controls framework (eg ISACA GDPR, ICO 10 Step, ISO 27001, or something similar) that can be used across both organisations to help maintain a robust level of ongoing compliance with the requirements of GDPR/DPA2018. See Key Recommendation Guidance on pages 21/22/23 for more information.	

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

<table>
<tr><th>Rec #</th><th>Issue</th><th colspan="2">Findings and Recommendation</th><th>Action Plan</th></tr>
<tr><td rowspan="2">7
(imp)</td><td rowspan="2"><u>Quality Management – Policies and Procedures</u>
Although it appears that policies, procedures are initially agreed across both organisations on final implementation they appear to deviate (eg Information Asset Register and Management Action Plans).</td><td colspan="2">Key findings
Comprehensive GDPR related management processes with supporting policies and procedures, across both organisations although sometimes different in content and approach. Published policies and procedures do not (always) have review periods specified and in some cases, are out-of-date eg SYPTE’s IT Policy.</td><td rowspan="2">Agreed Actions:
Agreed, annual review to be undertaken.
Responsible Officer:
Principal Solicitor
Executive Lead:
Steve Davenport
Due Date:
31/03/2021</td></tr>
<tr><td>7</td><td>Recommendation
Review the way GDPR/DPA2018 related policies and procedures are being managed across both organisations to ensure that they are remaining consistent and longer term, are capable of supporting closer integration should it be needed.</td></tr>
</table>

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
8 (imp)	Future Developments and Plans Whilst many of the building blocks of sound GDPR compliance are in place, it is not clear what the future intentions of the joint organisation are.	**Key findings** Authority consists of two separate legal organisational entities (SCRMCA and SYPTE) which should be treated as such and each be capable of being assessed at this time independently of the other, from a regulatory perspective. Evidence of cultural differences between the two organisations, which may present barriers to more efficient integration unless actively managed.		**Agreed Actions:** Agree, the two organisations are actively developing annual improvement plans to consistently improve compliance. Work on closer integration will continue. GDPR working group established. **Responsible Officer:** Stephen Batey and Andy Dickinson **Executive Lead:** Steve Davenport **Due Date:** ongoing
		8	**Recommendation** Consider using a GDPR maturity framework based approach across both organisations to assess where you are currently and what you are trying to achieve with your GDPR/DPA2018 compliance activities, particularly with regards to improving efficiencies and effectiveness. See Key Recommendation Guidance on page 24/25/26 for more information.	

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
9 (imp)	Compliance Management Automation The system being used is predominantly manual and therefore heavily labour focused, and dependent on interpretation of extensive data held in spreadsheets and other documents.	**Key findings** Each organisation uses a different Information Asset Register (IAR) format. SYPTE's IAR only contains a small subset of the fields used by SCRMCA, and does not clearly identify the associated Security Classification which should be used and other very important details which should be tracked and actively managed/maintained.		**Agreed Actions:** The two organisations will look at automation opportunities where they add value. **Responsible Officer:** Claire James and Andy Dickinson **Executive Lead:** Steve Davenport **Due Date:** 01/12/2020
		9	**Recommendation** Consider using a compliance management automation platform across both organisations (eg the Local Government Association's LG Inform Plus or something similar) to help you maintain your GDPR/DPA2018 compliance activities, particularly with regards to improving efficiencies and effectiveness. See Key Recommendation Guidance on page 27 for more information.	

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
10 (imp)	Log File Management With the exception of certain key conditions, the extracting of key insights and action events from activity log files is a manual process, which means that the investigation of certain suspicious events may be delayed or even missed.	**Key findings** Only basic operational type exception situations eg low disk are being automatically flagged in the log file related processes; suspicious non-operational based exceptional situations depend on manual review and escalation. It has not been possible to confirm, due to time constraints, whether system log files are appropriately secured and properly protected. System logs are not included on IARs.		**Agreed Actions:** Review to be undertaken and costings obtained. VfM assessment to be undertaken. **Responsible Officer:** Andy Dickinson **Executive Lead:** Steve Davenport **Due Date:** 31/03/2020
		10	**Recommendation** Review the way in which GDPR/DPA2018 related log file data is being used across both organisations to identify opportunities for the use of additional software to more easily alert relevant officials to abnormal and suspicious activity,	

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
11 (imp)	HR Platform Personal data (particularly, official-sensitive data) stored within the HR platform might not be protected in line with the requirements of DPA2018/GDPR, particularly with regards to access and physical protection.	**Key findings** SYPTE's HR platform know as WorldServices is being considered for replacement. However, it has not been possible to confirm how personal data (particularly, official-sensitive data) is being protected within the application, and the specific details of how access is being managed at a detailed level, from an application function security perspective, to ensure only an appropriate level of access is given based on the needs of a role.		**Agreed Actions:** New HR system being implemented. **Responsible Officer:** Rachel Radford **Executive Lead:** Steve Edwards **Due Date:** 30/09/2020
			Recommendation	
		11A	Review the way in which access to the HR platform is being managed by SYPTE, to ensure that access is being controlled and managed in line with the requirements of GDPR/DPA2018, and the associated information security classification of the data contained within the system.	
		11B	Review the way in which data within the HR platform (and associated non-production environments) is being protected, to ensure that it and in particular, official-sensitive designated data, is being properly protected in line with Cabinet Office and GDPR/DPA2018 requirements.	

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
12 (imp)	<u>Backup Data Protection</u> It has not been possible to confirm, due to time constraints, whether the backup data being held at the Barnsley Interchange is being properly protected and secured.	**Key findings** SYPTE's backup files are held offsite at the Barnsley Interchange, with a further backup in the cloud ie MS Azure based.		**Agreed Actions:** Agreed, increased security at Barnsley to be implemented. **Responsible Officer:** Nigel Cairns, Head of Infrastructure **Executive Lead:** Andy Dickinson **Due Date:** 01/10/2020
		12	**Recommendation** Review the way backup data is being protected to ensure that storage and access is in line with the requirements of GDPR/DPA2018 legislation.	

Action Plan

In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
13 (imp)	Internal Self-Auditing There are opportunities for each organisation to internally audit/review the others activities as a way of sharing views and best practice.	**Key findings** Comprehensive GDPR related management processes with supporting policies and procedures, across both organisations although sometimes different in content and approach. Also, there is also evidence of cultural differences between the two organisations, which may present barriers to more efficient integration unless actively managed.		**Agreed Actions:** GDPR working group established and meeting monthly to share best practice. **Responsible Officer:** Claire James and Andy Dickinson **Executive Lead:** Steve Davenport **Due Date:** 01/10/2020
		13	**Recommendation** Consider the use of an internal self-auditing approach that would enable each organisation to audit the other organisation's activities, to assist in sharing best practice and knowledge.	

Action Plan

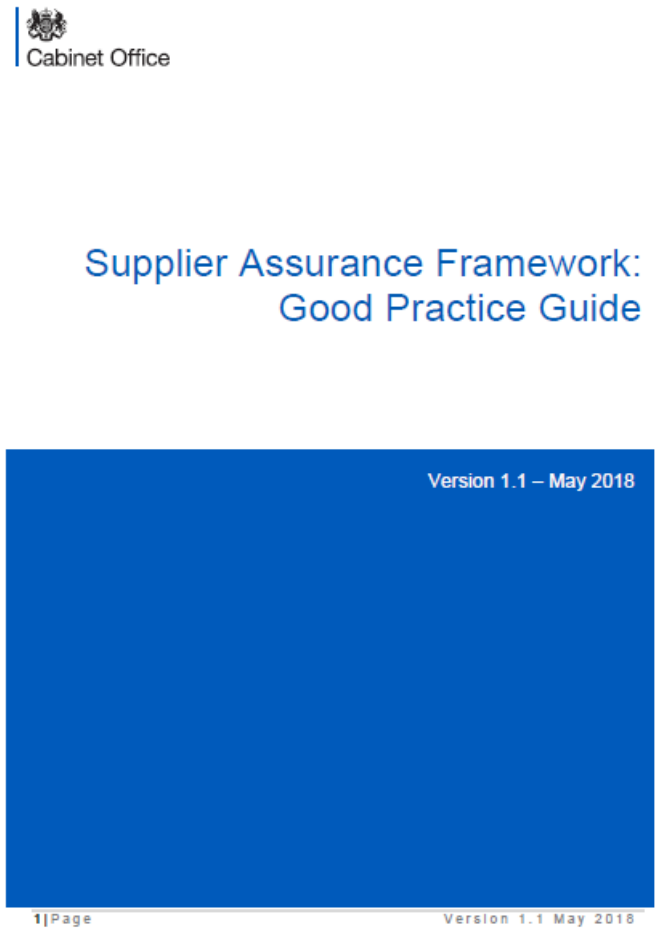
In this section we set out the findings arising from our work. We have organised the findings by recommendation rating. Details of what each of the ratings represents can be found in Appendix 3. NB Unless stated otherwise, our findings relate to both organisations ie the Authority and not to a specific organisation.

Rec #	Issue	Findings and Recommendation		Action Plan
14 (imp)	Unstructured Data Based on the details contained within the IARs for both organisations, there is a significant amount of personal data being held in unstructured locations.	**Key findings** SYPTE's IAR's show a significant amount of personal data that is destined for key systems such as the HR Platform, Payroll and the CRM applications, but is held temporarily in various unstructured locations whilst it is making its way to these structured repositories.		**Agreed Actions:** A new HR system will be implemented and further opportunities to review personal data flow across systems will be taken. **Responsible Officer:** Rachel Radford **Executive Lead:** Stephen Edwards **Due Date:** 30/09/2020
		14	**Recommendation** Review the way in which unstructured personal data is being used and stored across both organisations to ensure that it is always being securely protected, in line with the requirements of GDPR/DPA2018.	

Key Recommendations Guidance

Cabinet Office

Supplier Assurance Framework



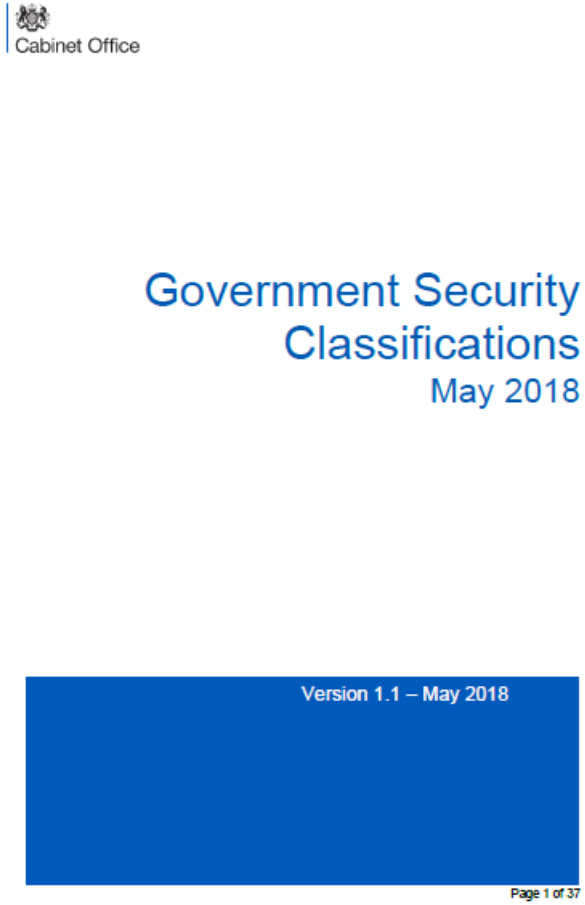
Source:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/707416/2018-May_Supplier-Assurance-Framework_Good-Practice-Guide.pdf

Key Recommendations Guidance

Cabinet Office

Government Security Classification



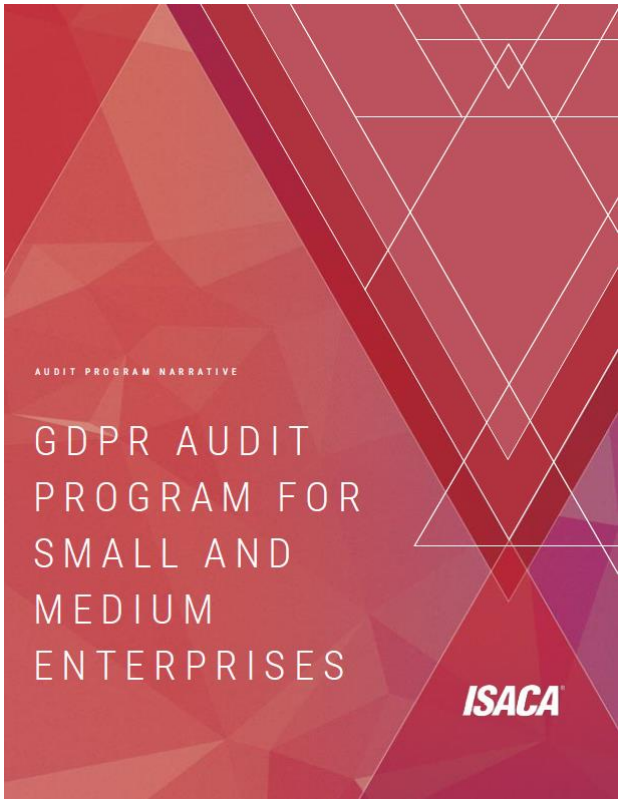
Source:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

Key Recommendations Guidance

Controls Framework

Ongoing Compliance Monitoring



GDPR Audit Program for Small and Medium-sized Enterprises
DPP1 Maintain Data Governance

Subprocess	Control Objectives	Referencing Articles	Controls	Testing Step	Ref. Framework/ Standards	Ref. Workpaper	Pass/Fail	Comments
DPP1.1 Establish DPP governance framework [M]								
DPP1.1 - 1	Governance is defined and documented with all key data protection responsibilities formally assigned.		Data protection and privacy (DPP) is a standing agenda item at the monthly board and management meetings.	1. Verify by inspection of the agenda and minutes of the board or management meeting.				
DPP1.1 - 2			The organization's operating activities are documented and include an assessment of their impact on DPP.	1. Verify that organizational objectives adequately reflect DPP provisions.				
DPP1.1 - 3			Formal documentation is in place to indicate regulatory requirements.	1. Review documentation for existence of procedures covering privacy, data collection, data handling, data retention, data security and data processing. 2. Verify that procedures contain appropriate references to frameworks and standards. 3. Verify that documentation contains review dates and authorization.				
DPP1.1 - 4			Formulating the organization's data protection policy has been assigned to a named individual or project group.	1. Review the responsibility assignment matrix (RACI) where completed. 2. Inspect the roles and responsibilities/job descriptions of those responsible for data privacy. 3. Interview the named individual.				
DPP1.1 - 5			There is a data protection policy in place and there are adequate procedures in place to ensure that the data protection policy is reviewed: a. periodically (e.g., annually)? b. amendments are subject to validation? c. amendments are made in a timely manner, i.e., immediately in the light of an actual event?	1. Confirm that the data protection policy was reviewed within the agreed timescale by checking the document's revision date, version number, etc. 2. Review the organization's data protection policy and confirm that it: • is clear and concise • explains the need for such a policy • states the organization's attitude towards data protection • clearly sets out the organization's data protection requirements • states the organization's data protection staffing and reporting structures • states the disciplinary procedures which may be invoked should employees fail to comply with the data protection policy				
DPP1.1 - 6			Objective and scope of the data protection "team," are adequately defined.	a. Confirm by examination that the objectives and scope of the data governance function (DGF), or equivalent, satisfactorily addresses data protection issues b. Check by enquiry that the make-up of the DGF includes representatives from: • senior management • appropriate users (e.g., units/sections) • the data protection officer (DPO) (if required or equivalent) • IT services • internal audit • legal services c. Examine the minutes of the group and note any specific issues, and confirm by enquiry that these were adequately followed up and addressed d. Review the reports made to, for example, the organization's directors and/or managing body and confirm that they are clear and accurately report the				

Instructions | Glossary of Terms | DPP1 | DPP2 | DPP3 | DPP4 | DPP5 | DPP6 | DPP7 | DPP8 | DPP9

Core Processes
DPP1 Maintain Data Governance
DPP2 Data Protection Responsibilities
DPP3 Manage Personal Data Risk
DPP4 Manage Personal Data Security
DPP5 Manage Personal Data Supply Chain
DPP6 Manage Incidents and Breaches
DPP7 Create and Maintain Awareness
DPP8 Organize DPO Function
DPP9 Maintain Internal Controls

Source: ISACA

Audit Programme: GDPR Audit Program for Small and Medium Enterprises:
https://www.isaca.org/bookstore/cobit-5/waugdpr

White Paper: Maintaining Data Protection and Privacy Beyond GDPR Implementation
https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpmdp

Key Recommendations Guidance

Controls Framework

Ongoing Compliance Monitoring

GDPR Audit Program for Small and Medium-sized Enterprises
DPP1 Maintain Data Governance

Subprocess	Control Objectives	Referencing Articles	Controls	Testing Step	Ref. Framework/ Standards	Ref. Workpaper	Pass/Fail	Comments
DPP1.1 Establish DPP governance framework [M]								
DPP1.1 - 1	Governance is defined and documented with all key data protection responsibilities formally assigned.		Data protection and privacy (DPP) is a standing agenda item at the monthly board and management meetings.	1. Verify by inspection of the agenda and minutes of the board or management meeting.				
DPP1.1 - 2			The organization's operating activities are documented and include an assessment of their impact on DPP.	1. Verify that organizational objectives adequately reflect DPP provisions.				
DPP1.1 - 3			Formal documentation is in place to indicate regulatory requirements.	1. Review documentation for existence of procedures covering privacy, data collection, data handling, data retention, data security and data processing. 2. Verify that procedures contain appropriate references to frameworks and standards. 3. Verify that documentation contains review dates and authorization.				
DPP1.1 - 4			Formulating the organization's data protection policy has been assigned to a named individual or project group.	1. Review the responsibility assignment matrix (RACI) where completed. 2. Inspect the roles and responsibilities/job descriptions of those responsible for data privacy. 3. Interview the named individual.				
DPP1.1 - 5			There is a data protection policy in place and there are adequate procedures in place to ensure that the data protection policy is reviewed: a. periodically (e.g., annually)? b. amendments are subject to validation? c. amendments are made in a timely manner, i.e., immediately in the light of an actual event?	1. Confirm that the data protection policy was reviewed within the agreed timescale by checking the document's revision date, version number, etc. 2. Review the organization's data protection policy and confirm that it: • is clear and concise • explains the need for such a policy • states the organization's attitude towards data protection • clearly sets out the organization's data protection requirements • states the organization's data protection staffing and reporting structures • states the disciplinary procedures which may be invoked should employees fail to comply with the data protection policy				
DPP1.1 - 6			Objective and scope of the data protection "team," are adequately defined.	a. Confirm by examination that the objectives and scope of the data governance function (DGF), or equivalent, satisfactorily addresses data protection issues b. Check by enquiry that the make-up of the DGF includes representatives from: • senior management • appropriate users (e.g., units/sections) • the data protection officer (DPO) (if required or equivalent) • IT services • internal audit • legal services c. Examine the minutes of the group and note any specific issues, and confirm				

Source: ISACA, Audit Programme: GDPR Audit Program for Small and Medium Enterprises
https://www.isaca.org/bookstore/cobit-5/waugdpr

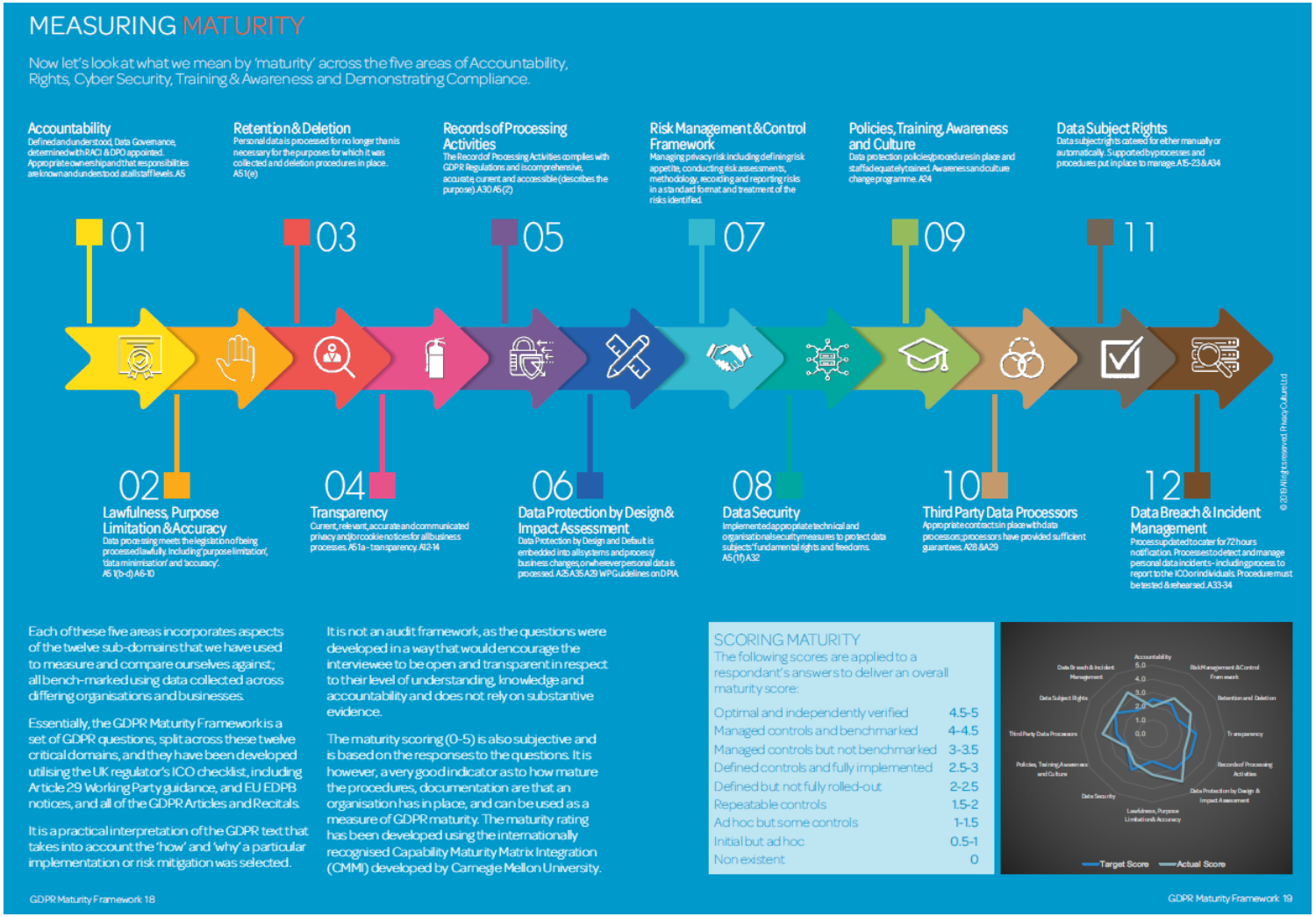
Key Recommendations Guidance

Controls Framework

Ongoing Compliance Monitoring

Next Steps	Further Information
	NCSC Ten Steps Cyber Control Framework: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security ISO/IEC 27001 Information Security Management Standard: https://www.iso.org/isoiec-27001-information-security.html NIST Cybersecurity Framework (CSF): https://www.nist.gov/cyberframework ISACA COBIT: http://www.isaca.org/COBIT/Pages/default.aspx CIS Critical Security Controls: https://www.cisecurity.org/controls/ Data Security and Protection Toolkit (DSPT), NHS Digital: https://www.dsptoolkit.nhs.uk/ Cyber Assessment Framework (CAF): https://www.ncsc.gov.uk/collection/caf ISACA GDPR Controls Framework: https://www.isaca.org/bookstore/cobit-5/waugdpr

Key Recommendations Guidance GDPR Maturity



Source: Steve Wright, Privacy Culture - https://iapp.org/media/pdf/resource_center/PrivacyCulture_GDPR_Maturity_Framework.pdf

MEASURING MATURITY

Now let's look at what we mean by 'maturity' across the five areas of Accountability, Rights, Cyber Security, Training & Awareness and Demonstrating Compliance.

01 Accountability
Defined and understood, Data Governance, determined with RACI & DPO appointed. Appropriate ownership and that responsibilities are known and understood at all staff levels. A5

02 Lawfulness, Purpose Limitation & Accuracy
Data processing meets the legislation of being processed lawfully, including 'purpose limitation', 'data minimisation' and 'accuracy'. A6 1(b-d) A6-10

03 Retention & Deletion
Personal data is processed for no longer than is necessary for the purposes for which it was collected and deletion procedures in place. A51(e)

04 Transparency
Current, relevant, accurate and communicated privacy and/or cookie notices for all business processes. A5 1a - transparency. A12-14

05 Records of Processing Activities
The Record of Processing Activities complies with GDPR Regulations and is comprehensive, accurate, current and accessible (describes the purpose). A30 A5 (2)

06 Data Protection by Design & Impact Assessment
Data Protection by Design and Default is embedded into all systems and process/ business changes, or wherever personal data is processed. A25 A35 A29 WP Guidelines on DPIA

07 Risk Management & Control Framework
Managing privacy risk including defining risk appetite, conducting risk assessments, methodology, recording and reporting risks in a standard format and treatment of the risks identified.

08 Data Security
Implemented appropriate technical and organisational security measures to protect data subjects' fundamental rights and freedoms. A5 (1f) A32

09 Policies, Training, Awareness and Culture
Data protection policies/procedures in place and staff adequately trained. Awareness and culture change programme. A24

10 Third Party Data Processors
Appropriate contracts in place with data processors; processors have provided sufficient guarantees. A28 &A29

11 Data Subject Rights
Data subject rights catered for either manually or automatically. Supported by processes and procedures put in place to manage. A15-23 & A34

12 Data Breach & Incident Management
Process updated to cater for 72 hours notification. Processes to detect and manage personal data incidents - including process to report to the ICO or individuals. Procedure must be tested & rehearsed. A33-34

Each of these five areas incorporates aspects of the twelve sub-domains that we have used to measure and compare ourselves against; all bench-marked using data collected across differing organisations and businesses.

Essentially, the GDPR Maturity Framework is a set of GDPR questions, split across these twelve critical domains, and they have been developed utilising the UK regulator's ICO checklist, including Article 29 Working Party guidance, and EU EDPB notices, and all of the GDPR Articles and Recitals.

It is a practical interpretation of the GDPR text that takes into account the 'how' and 'why' a particular implementation or risk mitigation was selected.

It is not an audit framework, as the questions were developed in a way that would encourage the interviewee to be open and transparent in respect to their level of understanding, knowledge and accountability and does not rely on substantive evidence.

The maturity scoring (0-5) is also subjective and is based on the responses to the questions. It is however, a very good indicator as to how mature the procedures, documentation are that an organisation has in place, and can be used as a measure of GDPR maturity. The maturity rating has been developed using the internationally recognised Capability Maturity Matrix Integration (CMMI) developed by Carnegie Mellon University.

SCORING MATURITY

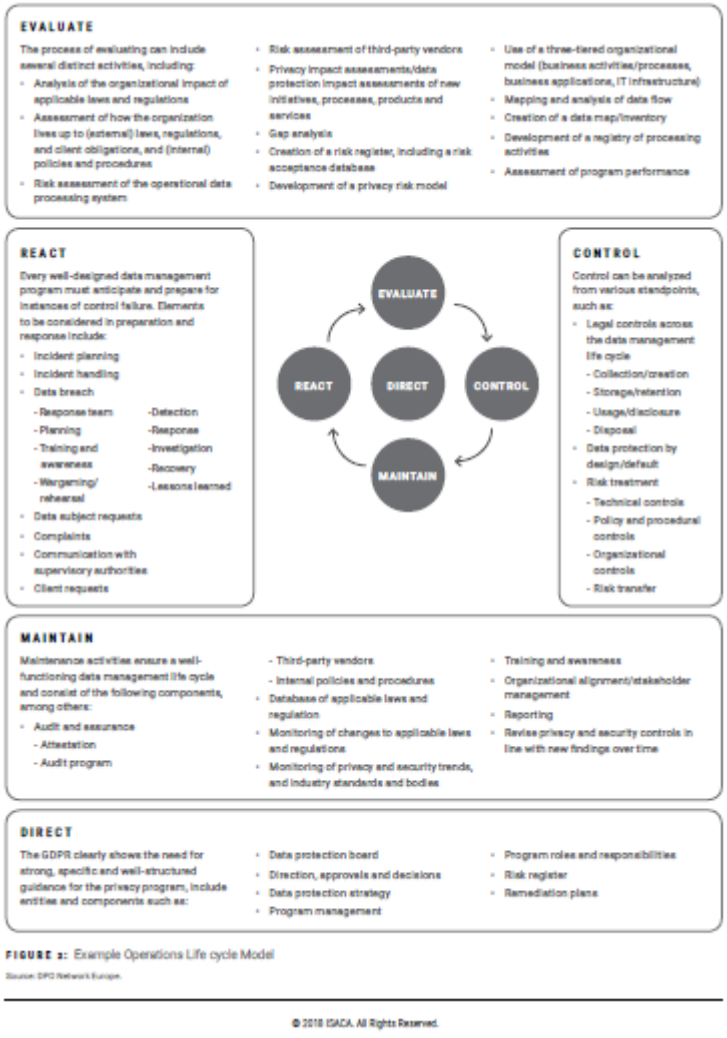
The following scores are applied to a respondant's answers to deliver an overall maturity score:

Optimal and independently verified	4.5-5
Managed controls and benchmarked	4-4.5
Managed controls but not benchmarked	3-3.5
Defined controls and fully implemented	2.5-3
Defined but not fully rolled-out	2-2.5
Repeatable controls	1.5-2
Ad hoc but some controls	1-1.5
Initial but ad hoc	0.5-1
Non existent	0

Source: Steve Wright, Privacy Culture

Key Recommendations Guidance
Other Guidance

Review and improve the existing controls and assurance framework to support current and future needs in the areas of information security including cyber security and data privacy (GDPR/DPA2018)



EVALUATE

The process of evaluating can include several distinct activities, including:

- Analysis of the organizational impact of applicable laws and regulations
- Assessment of how the organization lives up to (external) laws, regulations, and client obligations, and (internal) policies and procedures
- Risk assessment of the operational data processing system
- Risk assessment of third-party vendors
- Privacy impact assessments/data protection impact assessments of new initiatives, processes, products and services
- Gap analysis
- Creation of a risk register, including a risk acceptance database
- Development of a privacy risk model
- Use of a three-tiered organizational model (business activities/processes, business applications, IT infrastructure)
- Mapping and analysis of data flow
- Creation of a data map/inventory
- Development of a registry of processing activities
- Assessment of program performance

REACT

Every well-designed data management program must anticipate and prepare for instances of control failure. Elements to be considered in preparation and response include:

- Incident planning
- Incident handling
- Data breach
  - Response team
  - Planning
  - Training and awareness
  - Wargaming/ rehearsal
  - Detection
  - Response
  - Investigation
  - Recovery
  - Lessons learned
- Data subject requests
- Complaints
- Communication with supervisory authorities
- Client requests

EVALUATE
REACT
DIRECT
CONTROL
MAINTAIN

CONTROL

Control can be analyzed from various standpoints, such as:

- Legal controls across the data management life cycle
  - Collection/creation
  - Storage/retention
  - Usage/disclosure
  - Disposal
- Data protection by design/default
- Risk treatment
  - Technical controls
  - Policy and procedural controls
  - Organizational controls
  - Risk transfer

MAINTAIN

Maintenance activities ensure a well-functioning data management life cycle and consist of the following components, among others:

- Audit and assurance
  - Attestation
  - Audit program
  - Third-party vendors
  - Internal policies and procedures
- Database of applicable laws and regulation
- Monitoring of changes to applicable laws and regulations
- Monitoring of privacy and security trends, and industry standards and bodies
- Training and awareness
- Organizational alignment/stakeholder management
- Reporting
- Revise privacy and security controls in line with new findings over time

DIRECT

The GDPR clearly shows the need for strong, specific and well-structured guidance for the privacy program, include entities and components such as:

- Data protection board
- Direction, approvals and decisions
- Data protection strategy
- Program management
- Program roles and responsibilities
- Risk register
- Remediation plans

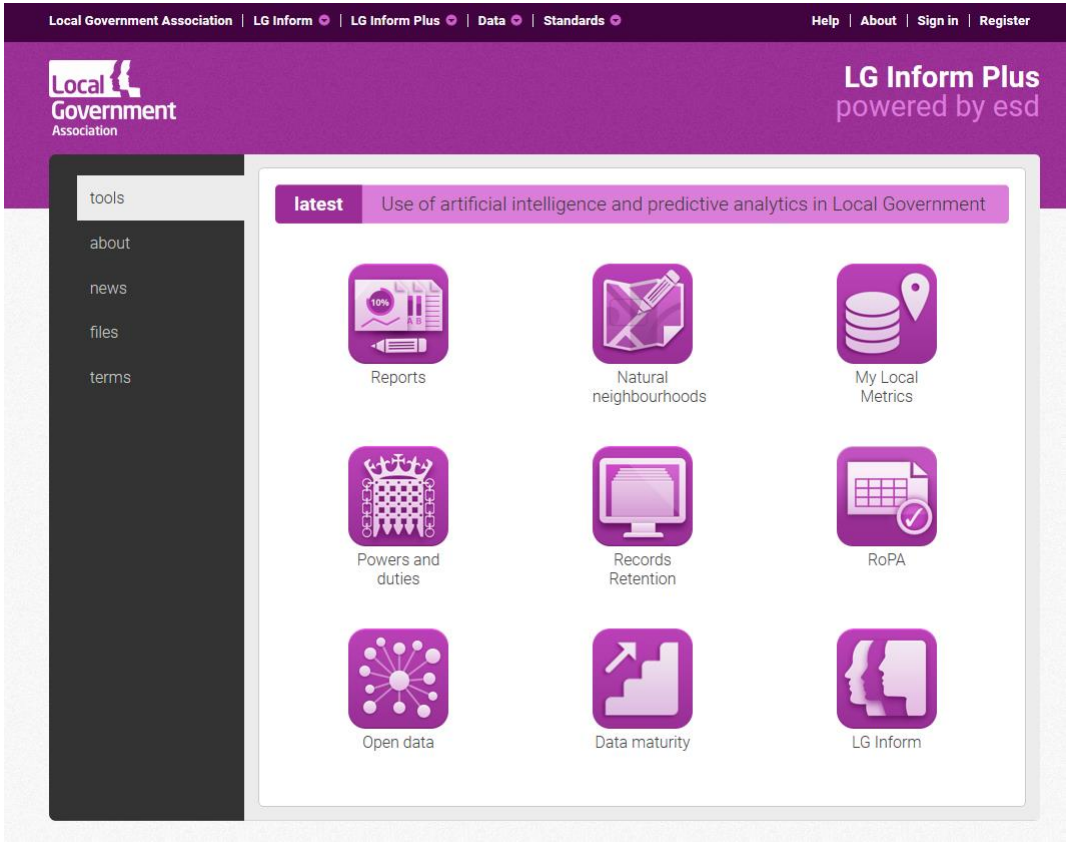
FIGURE 2: Example Operations Life cycle Model

Source: DPO Network Europe

Source: ISACA, White Paper: Maintaining Data Protection and Privacy Beyond GDPR Implementation https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpmdp

Key Recommendations Guidance Compliance System Automation

Example Only (and not official GT endorsement):
From the start of April 2018, LG Inform Plus offers enhanced data and tools to meet the General Data Processing Requirement (GDPR) to maintain a RoPA



Another good source of possible compliance solutions is the IAPP (International Association of Privacy Professionals) Privacy Tech Vendor Report: https://iapp.org/resources/article/2019-privacy-tech-vendor-report/

Source: Local Government Association - https://about.esd.org.uk/news/record-processing-activity-ropa-lg-inform-plus and https://about.esd.org.uk/tools

Appendices

Appendix 1
Audit Planning Brief

Internal

Presentation

Audit Planning Brief

General Data Protection Regulation - Internal Audit

Sheffield City Region Mayoral Combined Authority and South Yorkshire Passenger Transport Executive
November 2019

Appendix 2
Staff involved and documents reviewed

Staff involved

Steve Davenport - Principal Solicitor and Secretary (DPO) (Group)

Claire James - Senior Governance and Compliance Manager (SCRMCA)

Andy Dickinson - Head of Information Technology (SIRO) (SYPTE)

Stephen Batey - Head of Mayor's Office (SIRO)

Christine Marriott - Scrutiny Officer (SCRMCA)

Jayne Hampshire - Corporate Services (SYPTE) [check]

Scott Yellott - Corporate Services (SYPTE) [check]

Rachael Radford - Head of HR (SYPTE)

Documents reviewed

- Completed IASME-Governance-and-Cyber-Essentials-Question-Booklet
- Data Protection Policy
- Risk Management Policy
- IT Policy
- GDPR Policy Approval
- GDPR Compliance and Monitoring Plans
- GDPR Board Updates
- Privacy Impact Assessment Guidance
- Information Asset Assurance Process Procedures
- Data Breach Procedures
- Information Asset Registers
- Risk Management Data
- IT Health Check Reports

PLUS

- Other documents shared by Interviewees
- Documents downloaded from SCRMCA/SYPTE Public Website eg Public Trust Board Meeting Papers and other related NHS sites

Appendix 3 - Our assurance levels

The table below shows the levels of assurance we provide and guidelines for how these are arrived at. We always exercise professional judgement in determining assignment assurance levels, reflective of the circumstances of each individual assignment.

Rating	Description
Significant assurance	Overall, we have concluded that, in the areas examined, the risk management activities and controls are suitably designed to achieve the risk management objectives required by management. These activities and controls were operating with sufficient effectiveness to provide significant assurance that the related risk management objectives were achieved during the period under review. Might be indicated by no weaknesses in design or operation of controls and only IMPROVEMENT recommendations.
Significant assurance with some improvement required	Overall, we have concluded that in the areas examined, there are only minor weaknesses in the risk management activities and controls designed to achieve the risk management objectives required by management. Those activities and controls that we examined were operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review. Might be indicated by minor weaknesses in design or operation of controls and only LOW rated recommendations.
Partial assurance with improvement required	Overall, we have concluded that, in the areas examined, there are some moderate weaknesses in the risk management activities and controls designed to achieve the risk management objectives required by management. Those activities and controls that we examined were operating with sufficient effectiveness to provide partial assurance that the related risk management objectives were achieved during the period under review. Might be indicated by moderate weaknesses in design or operation of controls and one or more MEDIUM or HIGH rated recommendations.
No assurance	Overall, we have concluded that, in the areas examined, the risk management activities and controls are not suitably designed to achieve the risk management objectives required by management. Those activities and controls that we examined were not operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review Might be indicated by significant weaknesses in design or operation of controls and several HIGH rated recommendations.

Appendix 3 - Our assurance levels *(cont'd)*

The table below describes how we grade our audit recommendations.

Rating	Description	Possible features
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in the design or application of activities or control that requires the immediate attention of management	▪ Key activity or control not designed or operating effectively ▪ Potential for fraud identified ▪ Non-compliance with key procedures / standards ▪ Non-compliance with regulation
Medium	Findings that are important to the management of risk in the business area, representing a moderate weakness in the design or application of activities or control that requires the immediate attention of management	▪ Important activity or control not designed or operating effectively ▪ Impact is contained within the department and compensating controls would detect errors ▪ Possibility for fraud exists ▪ Control failures identified but not in key controls ▪ Non-compliance with procedures / standards (but not resulting in key control failure)
Low	Findings that identify non-compliance with established procedures, or which identify changes that could improve the efficiency and/or effectiveness of the activity or control but which are not vital to the management of risk in the business area.	▪ Minor control design or operational weakness ▪ Minor non-compliance with procedures / standards
Improvement	Items requiring no action but which may be of interest to management or which represent best practice advice	▪ Information for management ▪ Control operating but not necessarily in accordance with best practice