Towards a GDPR Compliance Assessment Toolkit

Sipho Ngobeni, Ntombizodwa Thwala, Nokuthaba Siphambili, Phumeza Pantsi, Bokang Molema, Jacob Lediga and Pertunia Senamela
Council for Scientific and Institutional Research, Pretoria, South Africa

sngobeni@csir.co.za
nthwala1@csir.co.za
nsiphambili@csir.co.za
ppantsi@csir.co.za
bmolema@csir.co.za
jlediga@csir.co.za
psenamela@csir.co.za

Abstract: The European Union's (EU) General Data Protection Regulation (GDPR) makes it illegal to collect, process, and store personal data unless it is done in accordance with the prescribed legal and regulatory clauses enshrined in the Act. Organisations face significant challenges in navigating GDPR requirements and assessing their level of compliance. In particular, failure to comply with GDPR may potentially expose the data Controller and Processor to steep legal penalties including possibly administrative fines of up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, which is imposed by the Supervisory Authority. This paper presents the results of a minimum viable product, the GDPR Compliance Assessment Toolkit (GCAT). The main objective of the GCAT is to assist organisations to assess their current state of compliance to GDPR. Drawing from an experimental research and development approach, GCAT is then compared with other existing GDPR compliance assessment technologies. Comparative analysis results shows that GCAT simplifies and optimize GDPR compliance assessments.

Keywords: GDPR, Privacy, Data Controller, Data Processor, Personal Data, Compliance Assessment

1. Introduction and Background

In this digital era, data has grown to be a valuable currency due to data being mined and processed to help make critical business decisions with the use of technology. The European Union (EU) introduced the General Data Protection Regulation (GDPR) Act which was enacted in April 2016 and came into effect in May 2018 (Zhuo et al, 2021). Similarly to the EU data protection regulation, GDPR recognises that individuals own and control their personal (but not contractual) data in perpetuity (Ke , 2024). This therefore suggest that individuals have rights to explicit consent (data opt-in), to be forgotten (data erasure), and portability (data transfer) (Ke and Sudhir, 2024). The main purpose of GDPR is therefore to protect individual personal data in terms of how it is collected, processed, and transferred to third parties (Kuner et al, 2021; Intersoft Consulting, 2021; Peukert et al, 2022 ; Ryngaert and Taylor, 2020; Vlahou et al, 2021). This law is applicable to European Economic Area (EEA)-based operations and certain non-EEA organisations that process personal data of individuals in the EEA. To date, GDPR has been reviewed and updated to version Article 97 which focuses on how data is transferred to third parties through the cross-border transfers and ensure there is co-operation amongst the organisations sharing the data.

The law is modelled to provide a set of requirements on how organisations should process personal data and the rules relating to the free movement of personal data. Since GDPR was enacted as law, it is now a legal compliance obligation. Most organisations are increasingly discovering the serious legal implications and challenges of achieving, demonstrating and maintaining mandatory compliance with GDPR are not as straight forward as they would have preferred, and panic is slowly creeping in. GDPR compliance is seen as exorbitant, intimidating, and complex; leaving many organisations unsure of how to tackle it. In addition, while its goal of empowering consumers and protecting their personal data is apparent, navigating its complexities can be difficult, particularly for enterprises in the midst of compliance efforts.

Data protection principles are concerned with how data is used lawfully, its purpose is stated and handled in a way that it is secure including the processing, destruction and recovery of the data. It is of utmost importance for organisations to specify what personal data will be used for, ensure data subjects have access to the data, and record how the data will be used, kept and failure to do so results in consequences. Furthermore, it is of utmost importance for organisations to take stock of the personal data they collect and share, and then put in place adequate controls to protect it. The legal consequences of non-compliance to this act will likely come from information security and privacy control deficiencies that relate to the processing and storage of personal data

and organisations not doing their due diligence in safeguarding personal information. It may also come as a result of gaps in policies and procedures that govern the handling of personal data. Failure to comply with certain provisions of GDPR may potentially expose the data Controller and Processor to steep legal penalties including possibly administrative fines of up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, which is imposed by the Supervisory Authority (Directorate-General for Communication, 2021).

Organisations need put their ducks in order when it comes to GDPR compliance, but many are now scrambling to tick the boxes and become compliant over-night. They have since realised the seriousness of non-compliance and the financial penalties thereof. Unfortunately, compliance to GDPR cannot be an over-night exercise. Organisations must invest time and money to be compliant. It is no secret that preparedness for GDPR compliance has become a top priority for most organisations, and more so as the enforcement deadline has come and passed. Therefore, the main purpose of this paper is to present the results of a technology demonstrator called GDPR Compliance Assessment Tool (GCAT). The GCAT is modelled through an experimental research and development approach. A comparative analysis of GCAT with other existing GDPR compliance assessment technologies is conducted. The result of the comparative analysis shows that GCAT simplifies and optimize GDPR compliance assessments.

2. Methodology

This paper followed an Experimental Research approach in order to implement the GDPR compliance assessment toolkit (Goddard, 2018). This is systematic work, drawing on the knowledge gained from research and practical experience and producing additional knowledge, which is directed to producing new products or processes or to improving existing products and processes. It this paper, we study several GDPR compliance assessment systems (both open-source and proprietary), with the aim to develop an improved system, called General Data Protection Regulation Compliance Assessment Toolkit. We then formulated performance metrics and used them to measure the performance of the proposed system against the existing systems.

The elements of the performance metrics (presented in Table 1) were formulated based on studying several existing Cybersecurity maturity metrics (Cybersecurity capability maturity model, 2022); (Privacy assessment maturity framework, 2014); (Hansen et al, 2016) including feedback from the pilots that were conducted . The metrics includes the following elements:

- **Compliance analysis and reporting** – this metric measures the capability of the system to take inputs from the entire assessment (compliant, not-compliant and non-applicable) and compute compliance/ non-compliance scores in a form of dashboards.
- **Provision of compliance maturity over time** – this criterion measures the ability of the systems to allow for organisations to mature their compliance over time and plot related maturity levels based on historical assessments. For example, determine compliance maturity ratings such as Non-existent (Level 0), Initial (Level 1), Defined (Level 2), Standardized (Level 3), Measured & Managed (Level 4 Optimized (Level 5).
- **User Management** – this criterion measures the ability of the system to ensure role-based access control. E.g, Assessor, Assessee and Approver. The segregation of duties is more important for quality assurance and audit purpose. One user cannot create and approve an assessment.
- **Provides prioritised areas of improvement based on top non-compliant categories** – this criterion measures the capability of the system to provide for an implementation roadmap for top non-compliance categories.
- **Provision of key focus areas where the organisation is compliant to GCAT** – this metric measures the capability of the system to determine overall compliance score taking into consideration all the sixteen assessed categories.
- **Provision of industry sector benchmarking** – this criterion measures the capability of the system to allow the assessed organisation to understand how they are currently doing in comparison to under industries within the same sector.

The results shows that the experimental development process yielded an improved system that performs or provides improved capability for organisation to self-assess their current state of compliance to the General Data Protection Regulation. A detailed presentation of the performance analysis using the metrics described above is presented in Section 5.

3. Results Analysis

The proposed system is a cloud-based solution that is used to assist organisations to evaluate their current state of compliance to the GDPR. These are organisations that collect, use, process or store personal data. The system can be accessed through a web browser on any device and consists of a file server, web server and database server. The system architecture was designed to ensure that components do not interfere with one another as depicted in Figure 1.

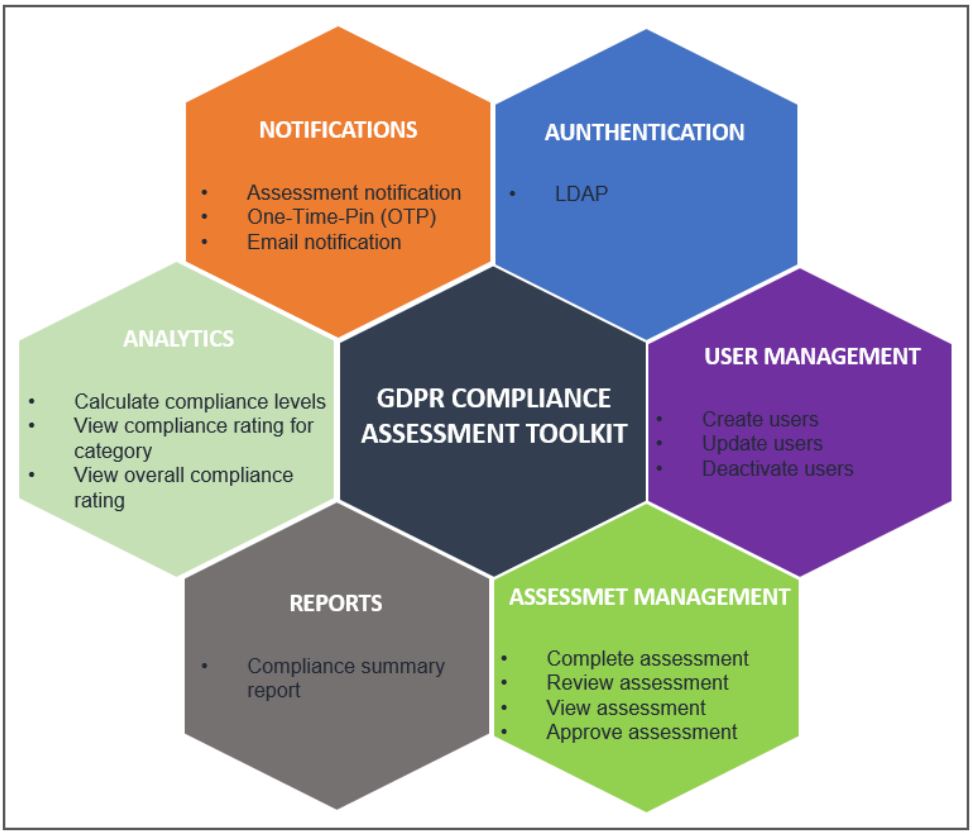

Figure 1: System architecture

The components of the system architecture are described below:

- **AUTHENTICATION** – the system requires users or the assessed organisation to submit their details to initiate the compliance assessment process. These details are then used to register the organisation, and representatives who will be taking the assessment.
- **USER AND ASSESSMENT MANAGEMENT** – the system uses role-based access control,

which include:

- **System Administrator** – adds organisation/s to be assessed in the system.
- **Assessor** – initiates the assessment evaluation process and sends the organisation's representative (Assessee) a link for completing a self-assessment.
- **Assessee** – completes the assessment on behalf of the assessed organisation.
- **Approver** – reviews and approves assessments.

- **REPORTING** – an executive summary report is generated for all approved assessments. The assessor will send this final report to Assessee upon approval.
- **ANALYTICS** – provides a results visualisation of the organisation's compliance
- posture.
- **NOTIFICATIONS** – provides assessment email notifications. To support these capabilities, the backend stores data in two forms, that is, a relational database using PostgreSQL and a File server to store the uploaded documentary evidence.

4. Development

The system allows an assessment to be created for an organisation as depicted in Figure 2. An organisation can complete one or more assessments, and each assessment can be completed by one or more representatives.

The system also makes provision for larger organisations to complete one assessment per business function. Once the various business functions complete their assessments, their individual compliance scores are then aggregated to form one compliance score for the entire organisation. Once an assessment(s) is created, the GCAT will automatically send the representative(s), herein referred to as Assessee, a link for the assessment. To access the GCAT the Assessee will be authenticated with a unique One-Time-Pin (OTP).

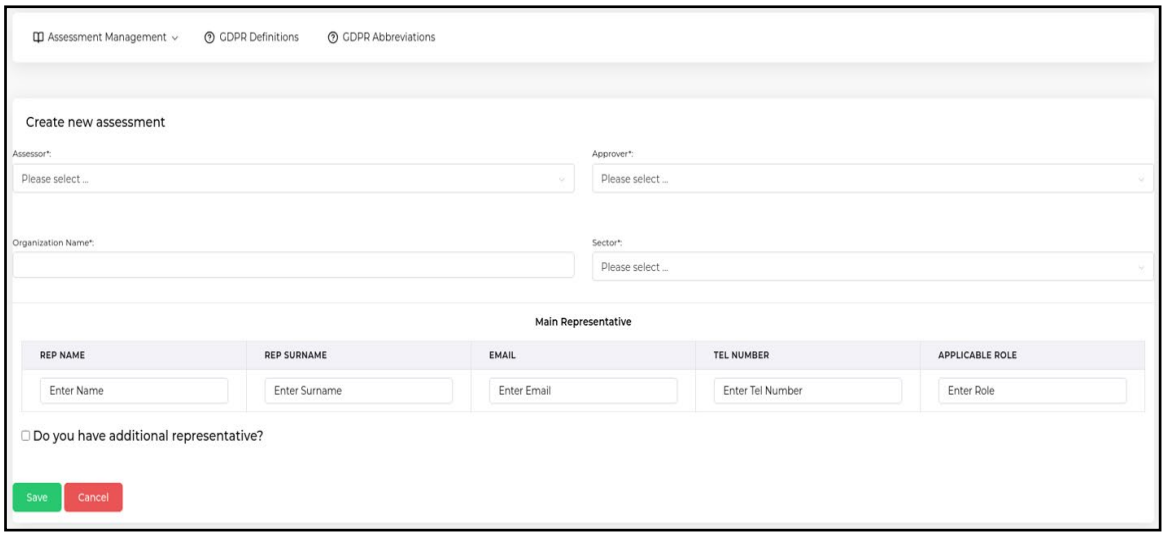

Figure 2: Creating an assessment for an organisation

Upon authentication the Assessee will be presented with a set of questions grouped into categories that align to the conditions defined in GCAT. In responding to each question, the Assessee will be able to provide comment and file-based evidence to support the compliance criteria selected (either Yes, No, or N/A) as indicated in Figure 3.

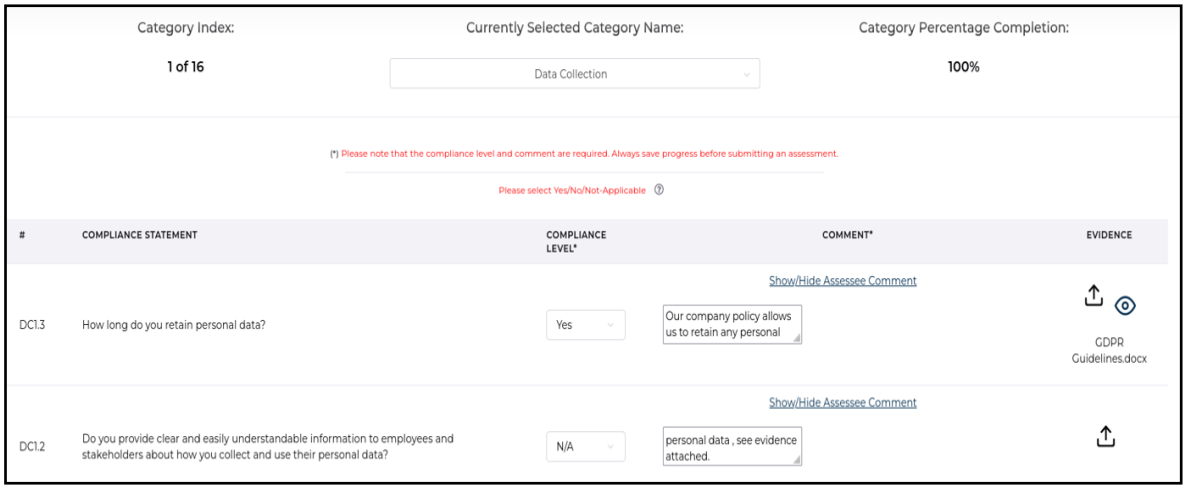

Figure 3: Assessment presented in a questionnaire format

On completion of the assessment the Assessee will receive notification that their assessment has been submitted for review. To assure quality of evidence and assessment results, the GCAT will route the completed assessment to an Assessor who will review and comment on the assessment. Once satisfied, the assessor will then submit the assessment to the Approver for finalization and approval (refer to Figure 4). Upon approval of the assessment the system will generate results of the assessment as depicted in Figure 5.

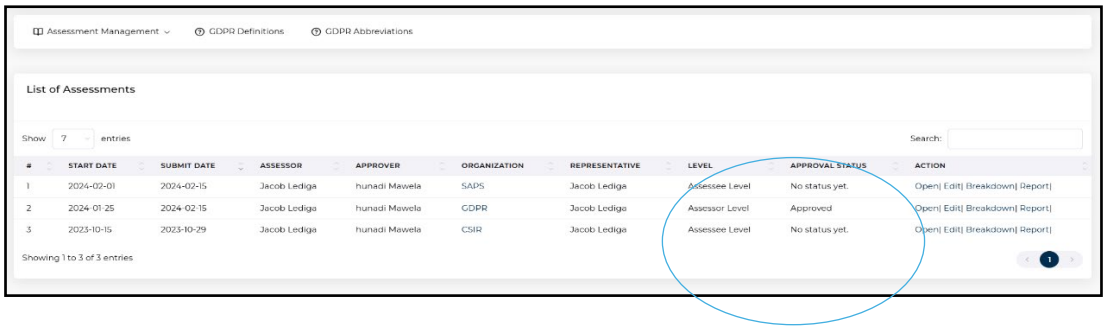

Figure 4: Quality assurance

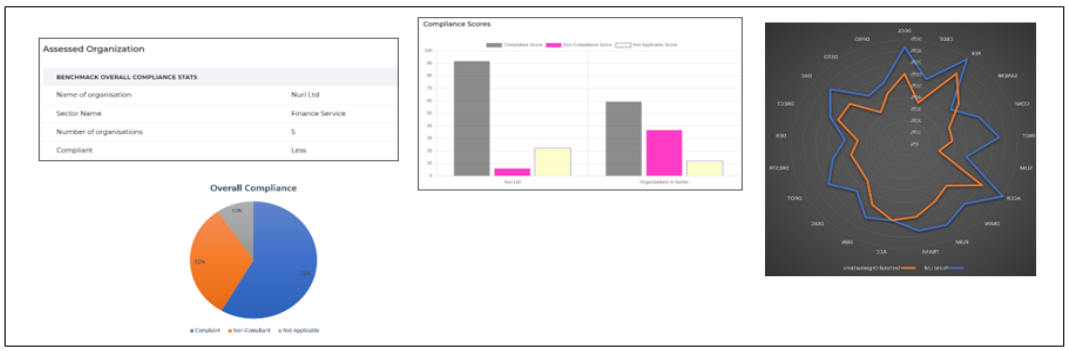

Figure 5: Results visualisation dashboards

5. Results

5.1 Performance Analysis

This research studied several GDPR compliance assessment toolkit such Wheelhouse GDPR Assessment tool (An Coimisiun um Chosaint Sonrai Data Protection Commission, 2022), CertiKit Limited GDPR gap assessment tool (CertiKit Limited, 2019), Sypher GDPR readiness assessment (Sypher, 2023), Nymity GDPR readiness questions (Nymity, 2019), Spirent Security labs GDPR compliance assessment (Spirent, 2018), CyberDefense GDPR compliance assessment (CyberDefense, 2023), Microsoft GDPR Accountability Readiness Checklist (Bernhardt et al, 2018), An Coimisiun um Chosaint Sonrai Data Protection Commission, and Report tool EU GDPR readiness assessment(ReportTool, 2018). Our study assessed the tools in terms of functionality and performance against set criteria described below. For the purpose of this paper, the following GDPR compliance assessment toolkit and the measured criteria were chosen:

- **Measured Criteria** – are measured against the existing systems.
- **Measured performance** – this is the optimal performance expected to be achieved by the proposed system and measured against the three existing systems.
- **GCAT** – this is the proposed GDPR Compliance Assessment Toolkit described in Section 3 and Section 4 above. The toolkit provides twenty-one compliance categories that are assessed while the rest of the compared existing toolkit does not provide comprehensive compliance categories.
- **Wheelhouse GDPR Assessment tool** – This is a GDPR assessment tool that provides feedback after answering the questions on each section of the GDPR. In addition, it provides recommendations on areas of improvement but does not provide compliance categories on data accuracy, Integrity and confidentiality.
- **CertiKit Limited GDPR gap assessment tool** – this is a complete set of forms, assembled and ready to use with an aim to guide an organisation through their GCAT compliance audit journey. Despite this, the tool does not provide compliance categories on data Integrity and storage limitation.
- **Sypher GDPR readiness assessment** – this system provides a GDPR assessment report after completing the system with areas of recommendations but does not provide compliance categories such as administrative fines and penalties.
- **Nymity GDPR readiness questions** – this is an excel sheet checklist template that continue to evolve to provide GDPR compliance but has many challenges regarding management of excel sheets as compared

to the proposed GCAT system. Similarly to the Sypher GDPR compliance assessment toolkit, it does not provide compliance categories such as administrative fines and penalties.

- **Microsoft GDPR Accountability Readiness Checklist** – this is a GDPR gap assessment took, it focuses on four compliance categories, that is, Conditions for Data Collection and Processing, Data Subject Rights, Privacy by Design and Default and Data Protection and security. The toolkit does not provide compliance categories on administrative fines and penalties and cross-border data transfers.

Table 1: Comparative analysis of GCAT and existing systems

Measured Criteria	Measured Performance	GCAT	Existing GDPR Compliance Assessment Tools				
			Wheelhouse GDPR Assessment tool	CertiKit Limited GDPR gap assessment tool	Sypher GDPR readiness assessment	Nymity GDPR readiness questions	Microsoft GDPR Accountability Readiness Checklist
Compliance analysis and reporting.	Generating analytics based on the compliance score and highlight GCAT Compliance Categories that need attention.	Provides analytics based on the compliance score and highlight GCAT Compliance Categories that need improvement.	Provides high level analytics based on categories only.	Provides high level analytics based on categories only.	Provides high level analytics based on categories only.	Provides high level analytics based on categories only.	Provides high level analytics based on categories only.
Provide compliance maturity level over time	The technology provides for organisations to mature their compliance over time and plot related maturity levels based on historical assessments.	Provide regulatory compliance maturity rating based on the levels: a) Non-existent (Level 0) b) Initial (Level 1) c) Defined (Level 2) d) Standardized (Level 3) e) Measured & Managed (Level 4) f) Optimized (Level 5)	No regulatory compliance maturity rating.	No regulatory compliance maturity rating.	No regulatory compliance maturity rating.	No regulatory compliance maturity rating.	No regulatory compliance maturity rating.
User management	Role-based access.	Provides for role-based access control, that is, System Administrator, Assessee, Assessor, and Approver.	Some elements of access management provided.	Some elements of access management provided.	Some elements of access management provided.	No role-based access management. Excel sheet.	Some elements of access management provided.
Prioritised implementation roadmap	Provide key focus areas for improvement.	Provides prioritised areas of improvement based on top non-compliant categories.	Not implemented.	Not implemented.	Not implemented.	Not implemented.	Not implemented.
Provide key performance indicators for	Provide key focus areas where the	Provides a prioritized key performance	Provides a prioritized key	Provides a prioritized key	Provides a prioritized key	Provides a prioritized key	Provides a prioritized key

Measured Criteria	Measured Performance	GCAT	Existing GDPR Compliance Assessment Tools				
			Wheelhouse GDPR Assessment tool	CertiKit Limited GDPR gap assessment tool	Sypher GDPR readiness assessment	Nymity GDPR readiness questions	Microsoft GDPR Accountability Readiness Checklist
the categories where the organisation is compliant to GCAT.	organisation is compliant to GCAT.	indicators for the categories where the organisation is compliant to GCAT.	performance indicators for the categories where the organisation is compliant to GCAT.	performance indicators for the categories where the organisation is compliant to GCAT.	performance indicators for the categories where the organisation is compliant to GCAT.	performance indicators for the categories where the organisation is compliant to GCAT.	performance indicators for the categories where the organisation is compliant to GCAT.
Provides industry sector benchmarking	Provides industry sectoral average compliance score of the assessed organisation.	Calculates and make provision for industry sectoral average compliance score for the assessed organisation.	Not implemented	Not implemented	Not implemented	Not implemented	Not implemented

Table 2 presents a summary of the performance results in Table 1 and a detailed discussion of the results is presented in Section 6.2. The legend "✓" depicts that the measured performance criteria is met and "✕"depicts that the measured performance is Not met, while "(✕)" depicts that the status is un-known.

Table 2: Summary of comparative analysis of GCAT and existing systems

Measured Criterial	Measured Performance	GCAT	Existing GDPR Compliance Assessment Tools				
			Wheelhouse	CertiKit	Sypher	Nymity	Microsoft
Compliance analysis and reporting.	Generating analytics based on the compliance score and highlight GCAT Compliance Categories that need attention	✓	✓	✓	✓	✓	✓
Provide compliance maturity level over time	The technology provides for organisations to mature their compliance over time and plot related maturity levels based on historical assessments.	✕	✕	✕	✕	✕	✕
User management	Role-based access.	✓	✓	✓	✓	(✕)	✓
Prioritised implementation roadmap	Provide key focus areas for improvement.	✕	✕	✕	✕	✕	✕
Provide key performance indicators for the categories where the organisation is compliant to GCAT.	Provide key focus areas where the organisation is compliant to GCAT.	✓	✓	✓	✓	✓	✓
Provides industry sector benchmarking	Provides industry sectoral average compliance score of the assessed organisation.	✕	✕	✕	✕	✕	✕

5.2 Discussion

This section is dedicated to the discussion of the performance analysis results presented in Section 5.1. can be noted from Table 1 that the GCAT is the most optimal solution compared to the five existing systems regarding:

- **Provision of compliance maturity over time** – this criterion measures the ability of the systems to allow for organisations to mature their compliance over time and plot related maturity levels based on historical assessments. In this instance, the GCAT outperforms the studied existing system because it provides a capability to determine compliance maturity ratings based on the following levels: Non-existent (Level 0), Initial (Level 1), Defined (Level 2), Standardized (Level 3), Measured & Managed (Level 4 Optimized (Level 5). All the other five existing systems does not provide regulatory compliance maturity ratings.
- **User Management** – this criterion measures the ability of the system to ensure role-based access control. It can be noted from Table 1 and Table 2 that the GCAT provides a capability for role-based access control, that is, systems administrator, assessor, assessee, and approver. While Wheelhouse, CertiKit, Sypher and Microsoft do provide some elements of access management, Nymity does not provide any access management, it is merely a spresheet and has many security implications including manual management of spreadsheet over time as compared to GCAT which is a web-based application.
- **Prioritised implementation road map** – this criterion measures the capability of the system to provide for an implementation roadmap after completing the assessment, that is, key focus areas for improvement. The GCAT provides this capability by making provision for prioritised areas of improvement based on top non-compliant assessment categories. All the other existing compared systems do not make provision for this capability.
- **Provision of industry sector benchmarking** – this criterion measures the capability of the system to allow the assessed organisation to understand how they are currently doing in comparison to under industries within the same sector. GCAT does provide a capability to calculate the average compliance score of the previously assessed organisations within the same sector as the currently assessed organisation.

6. Benefits of the GCAT System

The following are the benefits provided by the proposed GDPR Compliance Assessment Toolkit (GCAT):

- The most salient benefit is to assist organisations to assess their current state of compliance to GDPR.
- The system allows an organisation to complete one or more assessments, and each assessment can be completed by one or more representatives since various compliance categories could be require completion by representatives in different business functions.
- The system also makes provision for larger organisations to complete one assessment per business function. Once the various business functions complete their assessments, their individual compliance scores are then aggregated to form one compliance score for the entire organisation.
- The GCAT forms a basis from which other Cybersecurity governance and compliance assessment tools can be birthed from, e.g., compliance toolkit for ISO/IEC 27001 family of standards, privacy impact assessments, etc.
- The users of the GCAT are organisations in the private, public sector or EU member states. In addition, this tool could be used by organisations responsible for conducting audits for regulatory compliance.

7. Conclusion

The outcome of the GCAT system proposed in this paper showed that it was possible for an organisation to self-assess its current compliance posture against the GDPR requirements. This will then allow the assessed organisation to put together a road map for compliance based on the results provided by the system – areas of improvement. Future work entails creation of the executive summary report that forms part of the assessment results, which include the capability for this report to be also submitted via email to relevant representatives within an organisation. This does not necessary limit the key features of this tool, given that the Assessor and Approver already have access to the summary information for each organisation within the GDPR Compliance Assessment Toolkit. Furthermore, the toolkit will be improved to have a compliance assessment completion workflow that will include other role players within the assessed organisations to assist in the completion of the

assessment. The other role players may include Privacy Information Officer, Chief Information Security Officer, etc. In addition, an email notification functionality will be developed to inform the Assessee of any non-compliant resulting from the assessment.

References

An Coimisiun um Chosaint Sonrai Data Protection Commission. (2022) An Coimisiun um Chosaint Sonrai Data Protection Commission [Online]. Available at: https://www.dataprotection.ie/en/organisations/resources-organisations/self-assessment-checklist [Accessed: 13 October 2023]

Bernhardt, J, Mazzoli, R and O'Sullivan S. (2018) Microsoft GDPR Accountability Readiness Checklist [Online]. Available at: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-arc?view=o365-worldwide&culture=en-us&country=us [Accessed: 13 October 2023]

CertiKit Limited. (2019) CertiKit Limited [Online]. Available at: https://issuu.com/public-it/docs/gdpr-form-01-3_gdpr_gap_assessment_tool [Accessed: 15 September 2023]

CyberDefense. (2023) CyberDefense [Online]. Available at: https://www.orangecyberdefense.com/za/gdpr-compliance-assessments [Accessed: 5 November2023]

Cybersecurity Capability Maturity Model. (2022) US Department of Energy. [Online]. Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf [Accessed: 10 October 2023]

Directorate-General for Communication. (2021) *Rules for business and organisations, European Commission.* [Online] Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en [Accessed:14 February 2024].

Goddard, M. (2018) "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact", *International* Journal of Market Research, Vol. 59, No. 6, pp. 703-710.

Hansen, M., Hoepman, JH. and Jensen, M. (2016). "Towards Measuring Maturity of Privacy-Enhancing Technologies". Privacy Technologies and Policy. Lecture Notes in Computer Science, vol 9484. Springer.

Intersoft Consulting. (2021) *Intersoft Consulting.* [Online] Available at: https://gdpr-info.eu/ [Accessed 09 February 2024].

Ke, T. T. and Sudhir, K. (2024) "Privacy rights and data security: GDPR and Personal Data Markets", Management Science, Vol 69, No. (8), pp. 4389-4412.

Kuner, C., Bygrave, L.A., Docksey, C., Drechsler, L. and Tosoni, L. (2021) "The EU General Data Protection Regulation: A Commentary/Update of Selected Articles. Update of Selected Articles (May 4, 2021).

Nymity. (2019) Nymity GDPR Readiness questions [Online]. Available at: https://info.trustarc.com/Web-Resource-2019-01-19-Nymity-GDPR-Compliance-Toolkit_LP.html [Accessed: 12 October 2023]

Peukert, C., Bechtold, S., Batikas, M. and Kretschmer, T. (2022) "Regulatory spillovers and Data Governance: Evidence from the GDPR", Marketing Science, Vol 41, No. 4, p. 746–768.

Privacy Maturity Assessment Framework: Elements, attributes, and criteria. (2014) Online Available at: https://psi.govt.nz/privacyleadership/ [Accessed: 12 October 2023]

ReportTool. (2018). *Guidelines for Collecting and Reporting Data on Research and Experimental.* [Online] [Accessed: 23 November 2023].

Ryngaert, C. and Taylor, M. (2020) "The GDPR as global data protection regulation?", American Journal of International Law (AJIL)Unbound, Vol 114, p. 5–9.

Spirent. (2018) Sprirent SecurityLabs GDPR Compliance Assessment [Online]. Available at: https://assets.ctfassets.net/wcxs9ap8i19s/4XlBkiYtR7NN9xwczrKkom/920a2d6cdf473e8f543b5e2ee0518c2b/GDPR-Compliance-Assessment_whitepaper.pdf [Accessed: 13 October 2023]

Sypher. (2023) Sypher [Online]. Available at: https://www.sypher.eu/gdpr/assessment [Last Access: 25 September 2023]

Vlahou, A. Hallinan, D. Apweiler, R. Argiles, A. Beige, J. Benigni, A. Bischoff, R. Black, P.C. Boehm, F. Céraline, J. and Chrousos, G.P, (2021) "Data sharing under the General Data Protection Regulation: time to harmonize law and research ethics?", Hypertension, Vol 77, *No.* 4, pp.1029-1035.

Zhuo, R., Huffaker, B., Claffy, K. C. and Greenstein, S. (2021) "The impact of the General Data Protection Regulation on Internet Interconnection", Telecommunications Policy, Vol 45, No. 2, p. 102083.