SIS Security White Paper:

Managing privacy and security for the Service Information System

LogicalOutcomes

Authors:
Gillian Kerr, Ph.D., C.Psych.
Alberta Johnson
Sara Gaudon

With contributions from the LogicalOutcomes Ethics and Privacy Committee (Emilie Coyle, Valerian Marochko, Dave Montague, Neeran Saraf and Steven Uggowitzer) and other members of the LogicalOutcomes network (Moiz Azam, Sophie Llewelyn, Chintan Mehta, Martha McGuire and Roopang Mody).

Version: April 3, 2018
Permanent URL: https://doi.org/10.5281/zenodo.1211680

Contents

Introduction

The Service Information System (SIS) is a monitoring and evaluation platform built on open source software and donated Microsoft services that is offered on a subscription basis to nonprofits providing any kind of service. It is developed and managed by LogicalOutcomes, a Canadian nonprofit, and launched in March 2018. The first implementation was created in partnership with the Ontario Coalition of Agencies Serving Immigrants, funded by the Ontario Ministry of Citizenship and Immigration.

Features of SIS include surveys and other data collection tools, a data warehouse, a metadata registry of validated indicators, training videos, a community data portal containing public datasets, and customized evaluation sites with Power BI reports for each subscribing organization.

One of the main reasons we developed SIS was to protect the privacy of vulnerable people who are served by nonprofits. The responsible and secure use of personal data requires a great deal of ongoing effort and expertise, which most nonprofits are not equipped to provide. At the same time, nonprofits are expected by their funders to evaluate their services by collecting personal information from vulnerable clients. Our goal was to develop an effective monitoring and evaluation service that took care of most of the technical and administrative procedures, including security and privacy protections, so that nonprofits could focus on evaluation design and results.

This paper describes the security policies, principles and procedures that have been built into SIS to protect the privacy of personal information.

The audience for this paper includes SIS clients and users, LogicalOutcomes volunteers and consultants, and anyone else who wants to understand how we developed our security procedures.

SIS security principles

Even though SIS is funded by nonprofit organizations and their donors, personal data collected by SIS belongs to the individuals who provided the data, and must be handled in accordance with their consent. All of our security practices[1] are based on this simple assumption.

As a small non-profit organization that is staffed by international freelance consultants, LogicalOutcomes can't rely on long, complicated policies to assure the responsible use of data. Consultants simply won't read them. Furthermore, we don't have physical facilities that can be locked down, nor control over our contractors' computers, WiFi networks or workplaces. Some contractors share their computers with colleagues or family members, and many of them work out

[1] This paper emphasizes privacy, which is a subset of security. Security also includes the integrity and availability of information, which are also addressed in our procedures.

of their homes. We like the flexibility of this kind of work, but it requires deep thought about what we can feasibly deliver in the way of information security.

We settled on three sources of guidance for our security work.

1. Usability

In the context of a virtual organization working with collaborators who move in and out of projects, security processes must be easy to use, as unobtrusive as possible, and seen as valuable by team members. Otherwise they will be ignored. As Bruce Schneier writes, “People are the weakest link in the security chain”[2]. Security is part of a sociotechnical system that includes human behaviour as well as technical features.

We hire people who are interested in contributing their work to the community as open access or open source tools. Few of them want to spend time reading dense procedures. Usability means embedding good security practices within their LogicalOutcomes projects in a way that does not annoy them unnecessarily.

Therefore, as much as possible we have avoided writing documents that must be read by our regular consultants. Instead, we have tried to simplify procedures for users, and to make them fairly automatic through the configuration of project workspaces and tightly managed access controls (described below), saving complexity for internal auditors, administrators and security officers who actually need to know this stuff.

The overall policies that drive our security procedures are external sources that are widely known and highly credible: The nine Principles for Digital Development and the European Union’s General Data Protection Regulation (GDPR). A reliance on credible external sources that are relevant to the professional development of our consultants increases the likelihood that the security procedures will be followed.

2. Principles for Digital Development

The *Principles for Digital Development* were developed over many years by organizations and donors working in international development. Endorsers include UNICEF, WHO, UNDP, World Bank as well as many of the leaders in digital technology for development. They are:

1. Design With the User
2. Understand the Existing Ecosystem
3. Design for Scale
4. Build for Sustainability

[2] As cited in ‘Usable security: Why do we need it? How do we get it?’, Saase and Flechais, a book chapter of ‘Security and usability: Designing secure systems that people can use’, ed. By Cranor and Garfinkel, 2005. Article can be seen at https://pdfs.semanticscholar.org/0dc9/974f2c15c0a686881acb3eb5c1fa268bdc83.pdf

5. Be Data Driven
6. Use Open Standards, Open Data, Open Source, and Open Innovation
7. Reuse and Improve
8. Address Privacy & Security
9. Be Collaborative

The Principles are beautifully done, and well worth reading. For example, the section on Privacy and Security includes 10 core tenets, introduced by:

> *Organizations must take measures to minimize collection and to protect confidential information and identities of individuals represented in data sets from unauthorized access and manipulation by third parties. Responsible practices for organizations collecting and using individual data include considering the sensitivities around the data they have collected, being transparent about how data will be collected and used, minimizing the amount of personal identifiable and sensitive information collected, creating and implementing security policies that protect data and uphold individuals' privacy and dignity, and creating an end-of-life policy for post-project data management.*

The Principles acknowledge that privacy, while vital, is just one of the values that should drive digital development, and that we also have to ensure that our tools are driven by user needs, guided by user input, based on collaboration, and support open innovation.

These other values provide an important counter-balance to an overemphasis on secrecy. LogicalOutcomes is committed to creating open source and open access tools for social change. That commitment leads to a creative tension between the drive to share information freely and the responsibility to keep personal information confidential.

3. EU General Data Protection Regulation (GDPR)

The GDPR comes into force in May 2018, and will affect any organization offering services to European Union or United Kingdom residents or citizens, or that collects personal data from residents or citizens of the EU or UK, or has an office located within the EU or the UK.

The GDPR is all about giving individuals control over their own personal data. It is truly radical in its commitment to individual privacy, informed by bitter European experience with the use of personal information collected by Fascist and Soviet police states[3].

LogicalOutcomes has adopted the goal of GDPR compliance for our whole organization, including SIS as well as our consulting projects in evaluation and stakeholder engagement. For small organizations, GDPR requirements may be less stringent (this issue is being hotly contested in the EU and UK), and as a non-EU/UK organization we are not affected by national legislation related to

[3] See 'Unique European attitudes on data protection', p.22 and 'The East German Situation' in the 'Handbook of Personal Data Protection', p.87, Madsen 1992, at https://books.google.ca/books?id=BruxCwAAQBAJ .

GDPR, so we are using compliance aspirationally at this point. As GDPR practices become more mature we will continue to refine our procedures.

By complying with GDPR, we will also satisfy the requirements of Canadian privacy regulations, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Ontario Personal Health Information Protection Act (PHIPA)[4]. We also simplify discussions about how we protect the privacy of personal information we collect – we just refer to GDPR regulations and ask 'What do we need to do?'.

How we developed the privacy and security processes

Our security policies and procedures were developed by a group of volunteers, Board members and consultants at LogicalOutcomes, supported by an internal auditor who specializes in information security. They were overseen by an Ethics and Privacy committee of the LogicalOutcomes Board comprising representatives from our partner, OCASI.

We focused almost entirely on security within the Service Information System, ensuring that every aspect of our work with SIS incorporates privacy by design. Later, we applied the procedures to the entirety of LogicalOutcomes.

The development phases were as follows:

1. Initial policy development

The Ethics and Privacy Committee reviewed and contributed to initial drafts of a Responsible Data Policy based on Oxfam's excellent work[5] and an information security policy based on e-Health Ontario's[6]. We discussed our values and the principles that needed to underlie the security processes, and defined a workplan.

2. Asset and risk register

Sara Gaudon, Moiz Azam and Gillian Kerr developed a risk register listing every single information asset related to SIS. The register identified over 60 items capturing all the locations of potential personal information: chat logs, email services, consultants' computers, specific instances of each database, and so on. The register also included the names of each consultant involved in the development of SIS, as information assets within the system.

[4] I'm oversimplifying, of course. See a comparison of GDPR and PIPEDA at https://iapp.org/news/a/matchup-canadas-pipeda-and-the-gdpr/. To the extent that SIS and our evaluation projects rely on consent as the legal basis for data collection, GDPR is more demanding than PIPEDA.

[5] See https://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950

[6] See http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecPolicy_EN.pdf

Then we went over each asset to discuss the potential risks, threats and security controls that apply to each. This is a grueling process the first time you do it, but it's an essential step in controlling information.[7]

As we identified our assets and risks, they began to fall into simple categories that could be handled with group policies. We also saw how we could streamline our collaboration tools to reduce the number of services we need to manage and audit. Simply put, if an asset can't be audited it can't be controlled. So anything that we couldn't audit, or that is not being audited by a credible third party, was flagged as being problematic for sensitive personal information. That includes WiFi networks and computers used by our consultants unless they are in a locked and secured facility.

3. Selecting key GDPR compliance tools

One of the many benefits of adopting GDPR is the massive number of free resources that are available to help in the journey, as technology companies and governments scramble to get ready for the May 2018 deadline. After many weeks of reviewing compliance tools, we settled on two primary sources of GDPR information: The UK Information Commissioner's Office[8] and Microsoft's Compliance Manager[9].

We also identified training resources on research ethics (listed in the References section), a few encryption tools to provide enhanced protection for the most sensitive information, and guidance documents on the security of cloud-hosted personal information[10].

4. Updating policies and documentation

At this point, we went back to the initial policies drafted by the Ethics and Privacy Committee and simplified and updated them. For example, we discarded our Responsible Data Policy and replaced it with the *Principles for Digital Development*, described in the Principles section above.

We also wrote a new LogicalOutcomes privacy policy that incorporates GDPR requirements, and prepared this white paper to explain the thinking behind the procedures for anyone who wants a background and rationale.

[7] We used a horrendously complex risk register template that we don't recommend for general nonprofit use. Instead, consider the Threat Modelling asset register in 'The Hand-Book of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners and General Deportment', Responsible Data Program, 2016, p.27ff at https://responsibledata.io/resources/handbook/assets/pdf/responsible-data-handbook.pdf

[8] See https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/

[9] See https://servicetrust.microsoft.com/

[10] Key references included the new UK National Health Service guidance on requirements for offshore cloud hosting of personal health information (https://digital.nhs.uk/Offshoring-and-the-use-of-public-cloud-services) and a workbook on AWS compliance to German BSI IT Grundschutz, which has a large overlap with GDPR (https://d1.awsstatic.com/whitepapers/compliance/AWS_IT_Grundschutz_TUV_Certification_Workbook.pdf)

5. Testing and approval

Finally, we are in the stage of testing, implementing, revising and testing again. The policies and procedures will be reviewed by the Ethics and Privacy Committee and presented to the Board for approval in spring of 2018. They will be updated regularly.

The process of developing these policies, procedures and tools took far longer than we thought. The writer (Gillian Kerr) spent weeks investigating and testing procedures and then abandoning them when they turned out to be too expensive or unwieldy. We ended up with a set of procedures that we will now test and revise as necessary, returning to the principles above when we run into trouble.

Elements of SIS

Before getting into security, we'll pause to describe the elements of the Service Information System and how they fit together.

SIS is an integrated platform built on three open source programs (District Health Information System 2 [DHIS2], LimeSurvey and Aristotle MetaData Registry) and two Microsoft services (SharePoint and Power BI), supported by Office 365 collaboration tools (Microsoft Teams).

SIS databases are hosted by Amazon Web Services (AWS) and Microsoft Office 365 on Canadian servers. There are a few ancillary services like Zoho Desk for technical support, LastPass for password sharing, Cryptomator for client-controlled encrypted vaults and WordPress for the LogicalOutcomes web site, but SIS itself exists within the AWS and O365 environments.

As a general overview of the security architecture, personal information within the data warehouse (DHIS2) and survey data (LimeSurvey) are hosted on AWS Canadian servers, encrypted in transit and at rest with an encryption key that is managed by LogicalOutcomes.

Office 365 SharePoint sites and collaboration tools are encrypted and controlled according to policies that LogicalOutcomes has defined within Microsoft's Compliance Manager and SecureScore. Sensitive information within SharePoint (e.g., client email addresses that are used to send out surveys) will be encrypted with a passphrase that is not accessible to Microsoft, and we will offer the use of Cryptomator-encrypted vaults within OneDrive to protect highly sensitive files.

More information on SIS will be posted on the open access SIS community at https://zenodo.org/communities/sis. See the following mindmap for an overview of SIS elements:

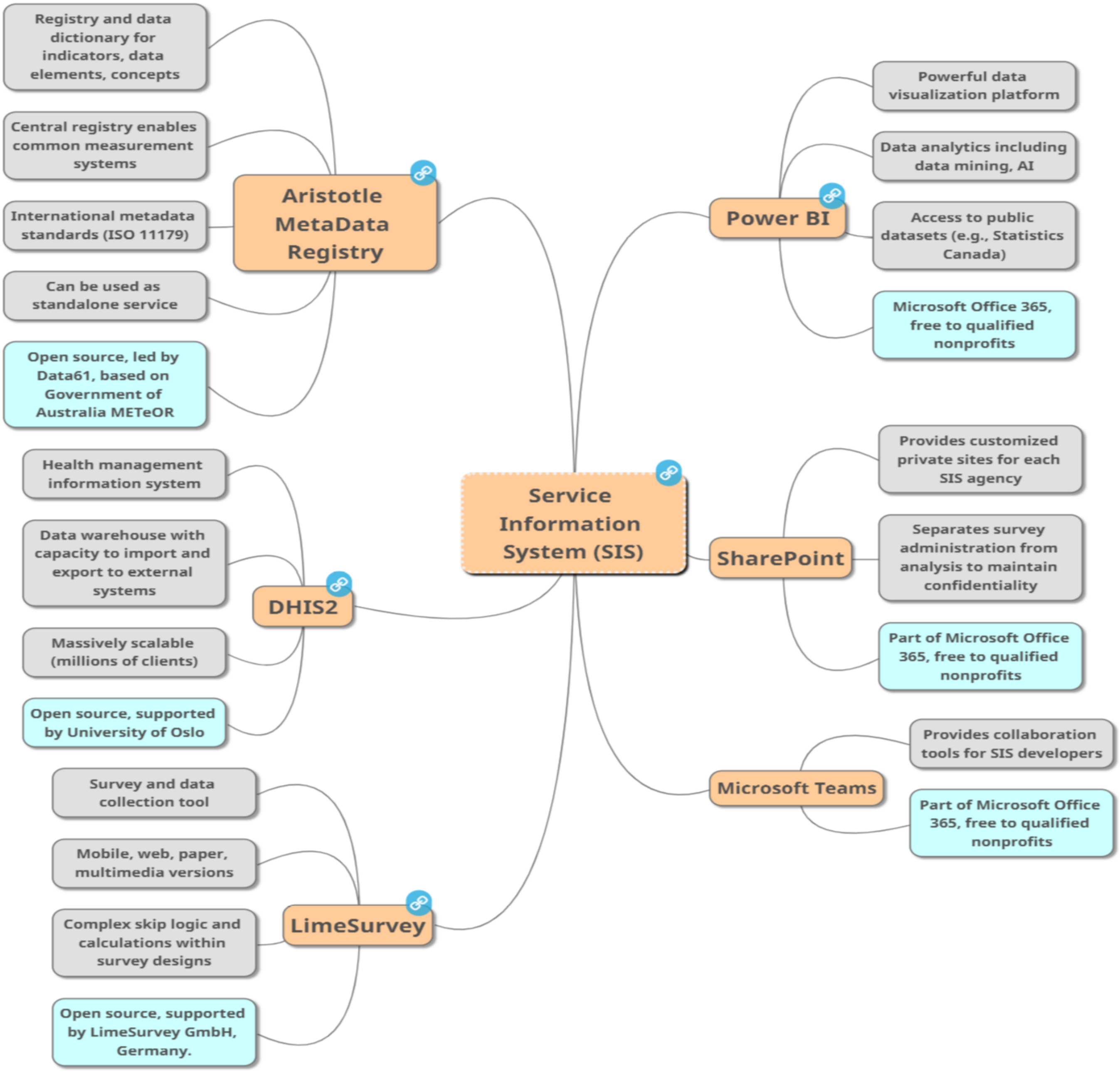

Registry and data dictionary for indicators, data elements, concepts
Central registry enables common measurement systems
International metadata standards (ISO 11179)
Can be used as standalone service
Open source, led by Data61, based on Government of Australia METeOR
Aristotle MetaData Registry
Power BI
Powerful data visualization platform
Data analytics including data mining, AI
Access to public datasets (e.g., Statistics Canada)
Microsoft Office 365, free to qualified nonprofits
Health management information system
Data warehouse with capacity to import and export to external systems
Massively scalable (millions of clients)
Open source, supported by University of Oslo
DHIS2
Service Information System (SIS)
SharePoint
Provides customized private sites for each SIS agency
Separates survey administration from analysis to maintain confidentiality
Part of Microsoft Office 365, free to qualified nonprofits
Microsoft Teams
Provides collaboration tools for SIS developers
Part of Microsoft Office 365, free to qualified nonprofits
Survey and data collection tool
Mobile, web, paper, multimedia versions
Complex skip logic and calculations within survey designs
Open source, supported by LimeSurvey GmbH, Germany.
LimeSurvey

Figure 1: Elements of the SIS platform

Our security framework

The simplest way to manage security processes is to create clear and consistent labels for information and then link each label with consistent policies.

We defined four labels that cover all the information assets that we create and manage:

- Open access
- Internal
- Confidential – Organization
- Confidential – GDPR

Each label is tied to a set of practices, so that LogicalOutcomes consultants don’t have to learn complex rules. We can create sub-labels with more fine-grained permissions if we need to, but it’s best to keep the categories few and simple.

Open access label

Whenever possible, we want to make our work products freely available to the community through Creative Commons licenses. If we have ownership of the products according to our consulting contracts and if the products are good enough to share, we will either post the products online ourselves or inform our contractors and colleagues that they can share the products with their own networks.

Internal label

Most of our information, by default, is labelled ‘Internal’. This means drafts, notes, background documents and reports that should not be publicly available but that would not cause serious harm to anyone if they were mistakenly shared with the wrong people (it might cause some embarrassment or affect the reputation of LogicalOutcomes as professionals). We do want to manage internal documents responsibly, but controls don’t need to be elaborate and expensive. Our priority is to encourage seamless collaboration between our clients and our consultants, and to reduce barriers to communication. When a project is finished, eligible work products will be re-labelled as ‘open access’ for sharing.

Confidential-Organization label

Some documents are highly confidential even if they don’t include personal information. Examples might include internal government policy documents, financial reports or corporate strategic plans. We ask client organizations to define the confidentiality level of their material at the project kick-off meeting, and then to work with us to ensure the documents are managed appropriately.

Confidential-GDPR label

Any information that is defined as personal under GDPR is given the GDPR label:

> *'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.*[11]

Explanation of security procedures

The security procedures are broken down by label: Open access, Internal, Confidential-Organization and Confidential-GDPR.

As usual, we will focus on privacy protection rather than the other two components of security (integrity and availability). Integrity and availability of LogicalOutcomes information is managed by Amazon Web Services and Microsoft Office 365, based on industry-standard backup policies defined by LogicalOutcomes. For more information, see our separate GDPR Compliance report, which will be posted in the Zenodo SIS community.

An overview of our security procedures is summarized in the mind map below. You can expand the image or go to the up-to-date online version[12], where you will see links to the key resources.

[11] GDPR, Article 4. See https://gdpr-info.eu/art-4-gdpr/

[12] See https://atlas.mindmup.com/gilliankerr/security_processes

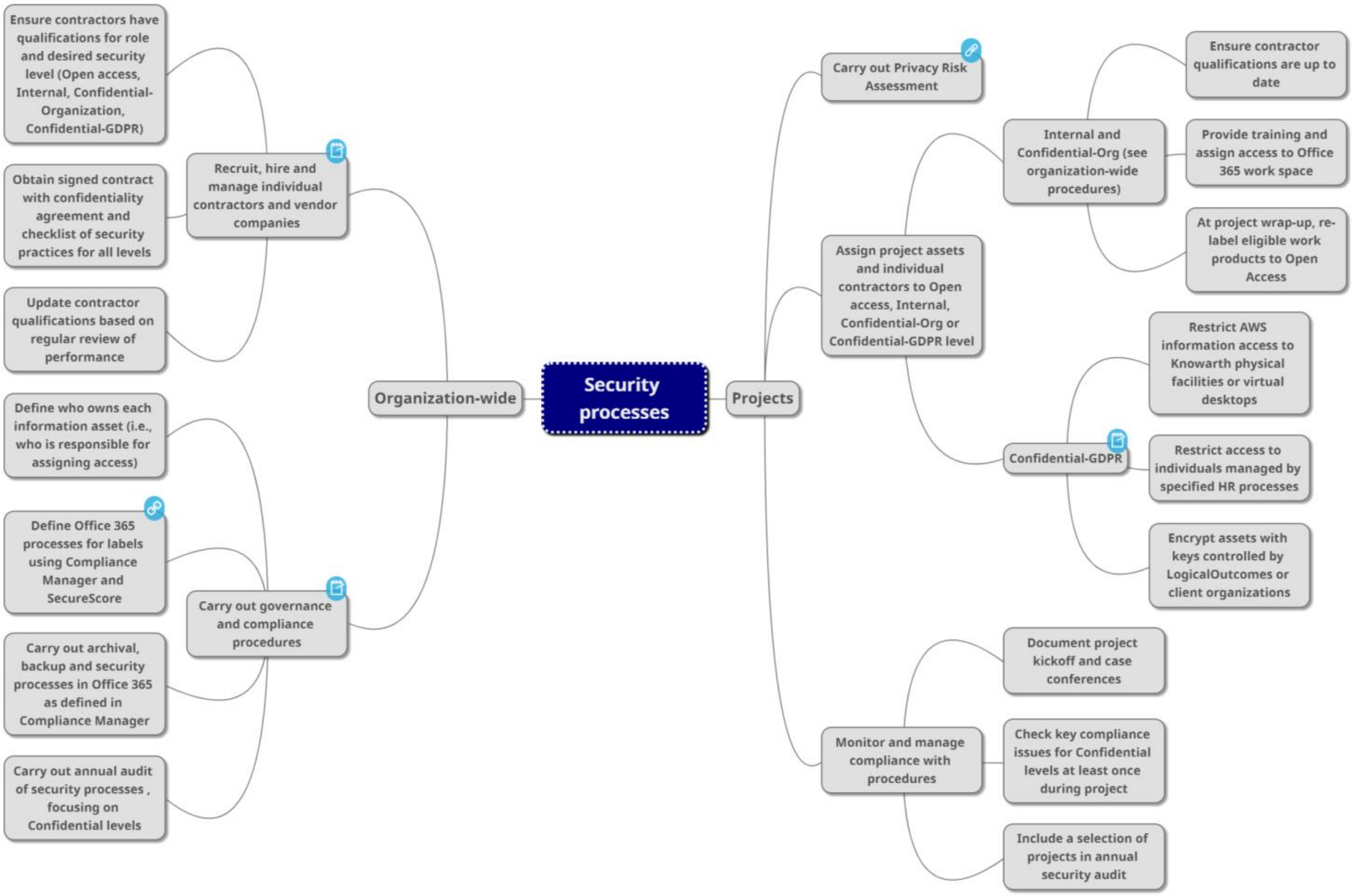

Security processes
Organization-wide
Recruit, hire and manage individual contractors and vendor companies
Ensure contractors have qualifications for role and desired security level (Open access, Internal, Confidential-Organization, Confidential-GDPR)
Obtain signed contract with confidentiality agreement and checklist of security practices for all levels
Update contractor qualifications based on regular review of performance
Carry out governance and compliance procedures
Define who owns each information asset (i.e., who is responsible for assigning access)
Define Office 365 processes for labels using Compliance Manager and SecureScore
Carry out archival, backup and security processes in Office 365 as defined in Compliance Manager
Carry out annual audit of security processes , focusing on Confidential levels
Projects
Carry out Privacy Risk Assessment
Assign project assets and individual contractors to Open access, Internal, Confidential-Org or Confidential-GDPR level
Internal and Confidential-Org (see organization-wide procedures)
Ensure contractor qualifications are up to date
Provide training and assign access to Office 365 work space
At project wrap-up, re-label eligible work products to Open Access
Confidential-GDPR
Restrict AWS information access to Knowarth physical facilities or virtual desktops
Restrict access to individuals managed by specified HR processes
Encrypt assets with keys controlled by LogicalOutcomes or client organizations
Monitor and manage compliance with procedures
Document project kickoff and case conferences
Check key compliance issues for Confidential levels at least once during project
Include a selection of projects in annual security audit

Figure 2: Mind map of LogicalOutcomes security procedures

1. Organizational vs project security

The security mind map is divided between organization-wide procedures, which apply to everything we do, and project-based procedures, which are based on a privacy risk assessment that is done at the beginning of each project.

Organization-wide procedures cover our human resources practices – recruiting, hiring, training and managing – as well as the configuration of our Office 365 environment and our auditing procedures. Human resources are covered in its own section below.

Everything else is done at the project level, which is appropriate for a project-based consulting organization.

2. Privacy risk assessments

The Project Manager for each project, whether internal or external, is responsible for assessing whether the project will handle personal information. We have adapted the risk framework developed by the UK National Health Service for use in the risk assessment.[13]

If the project is handling personal information according to the risk framework, those assets are labelled and managed according to the Confidential-GDPR procedures described below. SIS does include personal information – see the SIS privacy risk assessment in the appendices.

The Project Manager then assesses, in collaboration with the client organization, whether any project information assets are in the Confidential-Organization category. *This decision is made by each organization based on its own risk assessment and comfort level.* Generally, even within a sensitive project, most documents will be labelled as 'Internal', with a few documents labelled as Confidential-Organization. The question to ask when deciding on labels is whether an organization or its members would be harmed if information is shared with the wrong people. This decision is made during the approval of the Project Charter if not before.

3. Open access procedures

Wherever possible, we share our work products with the community through Creative Commons licensing. This approach actually improves security by encouraging open discussion among our clients and contractors about what we can make shareable. Otherwise, and understandably, contractors tend to secretly keep copies of their own work that they can re-use in other projects. This creates unnecessary ethical pressures on the sector, makes security compliance difficult, and prevents open sharing.

In our consulting contracts, we ask that work products we develop be jointly owned or shared with LogicalOutcomes and the client organization. We have posted suggested wording in a contract template that has been reviewed by many NGOs in Canada, the US and elsewhere[14].

We try to post useful materials to Github and/or Zenodo, to make them easy to find, use and cite. And we will be encouraging consultants and colleagues to link their contributions to their personal ORCID Contributor IDs, to facilitate attributions[15].

For projects that are aimed solely at creating open access products, we create Microsoft Teams using the most open collaborative settings. Each project member may add new members, and

[13] See https://digital.nhs.uk/article/8489/Health-and-social-care-data-risk-model- and the associated guidelines at https://digital.nhs.uk/article/8488/Health-and-social-care-cloud-risk-framework

[14] See https://doi.org/10.5281/zenodo.1197223

[15] For example, Gillian's ORCID ID is http://orcid.org/0000-0002-7300-9706, and it's automatically linked to all of her Zenodo contributions. We want to encourage the practice of acknowledging contributions to open access knowledge.

may add external applications and bots within the Team environment. However, project information is labelled as Internal until the documents or tools are ready to share publicly.

Note that there may be Confidential-GDPR assets that are related to an Open Access project, such as the development of the SIS platform itself. Anything labelled with Confidential-GDPR is handled according to the GDPR procedures. For example, a separate Microsoft Team would be created to handle GDPR-related material, and kept separate from an Open Access Team.

4. Internal procedures

Most of our information, by default, is labelled Internal. We use collaboration-friendly configurations for Microsoft Teams and SharePoint libraries, such as allowing external users, and not forcing multi-factor authentication.

Most of our security controls are based on Office 365's access permissions and rely on the professionalism of the contractors we hire. Essentially, we try to recruit good, ethical people who act professionally and responsibly, and monitor their adherence to our Human Resources policies (below).

5. Confidential-Organization procedures

During the approval of the Project Charter[16] or before, we will ask our client organization to define whether any of their information should be labelled Confidential-Organization. LogicalOutcomes may also label their own documents as Confidential-Organization. The label is up to each organization based on their own assessment of risk.

For example, at LogicalOutcomes we define administrator passwords as Confidential-Organization. Passwords to services like our website are stored and shared in LastPass. Access to Office 365 resources are protected through multifactor authentication and a requirement that users do not share accounts. Shared accounts make logging and auditing very difficult and are poor practice for confidential information.

Note that Internal projects may contain Confidential-Organization folders. Labels are applied at both the project and folder level, at the beginning of the project, by the Project Manager.

Once a Confidential-Organization label has been applied to a folder, the Project Manager will decide which protections should be applied. By default, a Confidential-Organization folder places restrictions on whether a document can be copied or forwarded. Even if the document is accidentally forwarded in an email, it cannot be opened unless the recipient has been given explicit permission by the owner.

[16] The project charter can also be called the statement of work or the project terms of reference.

For even higher sensitivity, folders can be kept inside a Cryptomator vault. Cryptomator is open source encryption software that enables document synchronization within OneDrive while maintaining an encryption key that is controlled by the owner. It cannot be accessed by Microsoft.

In our experience, client organizations find tight security controls irritating and generally not worth it. However, if a client organization wants to implement extra protection we have the means to do it.

6. Confidential-GDPR procedures

Unlike 'Confidential-Organization', which is defined by the client organization and managed jointly with LogicalOutcomes, the GDPR category of information is tightly controlled by LogicalOutcomes. We do not share sensitive GDPR information with client organizations without the consent of the data provider (e.g., the survey respondent).

These procedures are the most elaborate. In summary:

- Project meetings and collaboration tools (such as Microsoft Teams, emails and chat) must never include any personal information about a respondent. We ensure this by restricting access to individual-level personal information to a very small group of trained analysts and developers whose access is logged and audited.

- Individual-level personal information, in which someone's identity could be figured out through data mining, is stored in a DHIS2 data warehouse. It is hosted by Amazon Web Services on Canadian servers, encrypted at rest and in transit using an encryption key that is inaccessible to AWS.

- Survey data collected in LimeSurvey is deleted shortly after being passed through to DHIS2 for storage. The LimeSurvey database, like the DHIS2 database, is on AWS Canadian servers and encrypted with a key inaccessible to AWS.

- The DHIS2 and LimeSurvey databases are managed by Knowarth Technologies, our hosting partner. Their hosting configuration is described in the appendices, and follows the recommendations for cloud-hosted personal health information recently published by the UK National Health Service.

- Aggregate data is passed from DHIS2 to a tightly controlled Power BI workspace through an API connection, encrypted in transit. In other words, instead of sending a response from a Kenyan woman aged 22, DHIS2 would transfer information about responses from women ages 19 to 24 from Africa. This reduces the possibility of identifying any one person. Open-ended comments (such as 'suggestion boxes') are not aggregated (though they are not tied to any demographic information), and there is some risk of recognizing a respondent by what they say. This risk is pointed out in the survey consent form, and respondents may leave those questions blank. SIS organizations may choose not to include open-ended questions in their surveys.

- Our Power BI analysts are mainly data scientists at CloudsonMars[17], our analytic partner. They are managed according to human resources policies described below, and are trained in privacy and confidentiality. Unless given specific consent by SIS organizations, these analysts will not see individual-level personal information.
- If SIS organizations wish to carry out detailed analyses, including data mining and qualitative analyses of responses linked to demographics, they may hire LogicalOutcomes or CloudsonMars data analysts or contract with their own. SIS will make the individual-level data available to those analysts under the conditions that (1) it is allowed by the original consent from the respondents, (2) the analysts have been qualified by a national statistical agency or research university to study sensitive personal data, and (3) the analysts follow the access procedures described next.
- Data analysts who are working directly with individual-level personal information must access it via a virtual Windows desktop hosted by Knowarth Enterprises from within their secure facility. Each analyst will have a separate username and will require to use multifactor authentication to log in. They must save working files in encrypted Cryptomator vaults within the virtual workspace, and promise not to copy the material outside the vaults. By using virtual desktops and multifactor authentication, we are, in a sense, providing analysts with a locked and secured physical facility.
- Data analysts will share results and summaries with the SIS organizations who have contracted their services, but may not share the raw data.
- SIS organizations are welcome to screen the individual analysts who work with their data by reviewing their bios and talking to them directly.

So far, we have described the procedures for the data warehouse and survey databases. There is also some personal information within SharePoint and Power BI. The procedures for Office 365 include:

- All Office 365 documents and lists are encrypted in transit and at rest. For sensitive aggregate information, such as reports that might stigmatize client groups as a whole, SIS can add additional protection against copying and forwarding information to the wrong people.
- Any files that contain personally identifiable information (PII), such as email addresses or other contact information for clients, can be stored in encrypted vaults with keys that are controlled by the SIS organization. These keys are not accessible by Microsoft and would not be accessible to any warrant or subpoena from the U.S. government.

[17] http://cloudsonmars.com/

- For SharePoint lists that include personally identifiable information (PII), such as email addresses for sending out surveys, SIS will encrypt the fields containing the PII. (This feature is in development and will be introduced in mid-2018.) The email addresses will not be associated with any responses. If a SIS organization prefers, they can send emails to respondents directly through their own email service rather than through SIS.

7. Human resources policies for contractors and partners

The most important security controls – and risks – are the people who implement them. We choose our consultants and partners carefully, and control their access to confidential information.

LogicalOutcomes

LogicalOutcomes has no employees. We are all contractors, working all over the world, collaborating on Microsoft Teams and other online tools.

When we hire, we almost always have access to reviews from previous employers either through UpWork ratings or through our personal network. We review bios to check that contractors have the experience relevant to their role, and monitor their performance. At the end of each project, the Project Manager evaluates each contractor in terms of their fit with our values and potential for future work.

Each contractor signs a confidentiality agreement and a commitment to follow certain basic security processes in working with LogicalOutcomes information (see appendices).

Contractors working with Confidential information are screened even more carefully, and are required to use multifactor authentication to access Confidential assets. Access to GDPR individual-level information is restricted to very few people, only for specified functions, and their interactions with personal-level data are logged and audited monthly.

For people in certain key roles, we independently verify qualifications. For example, certifications for Certified Information Security Manager (CISM) and Certified Information System Auditors (CISA) can be verified on ISACA's web site, and ISACA's certification processes themselves are audited by the American National Standards Institute (ANSI).[18] Gillian Kerr, who leads the Ethics and Privacy Committee of SIS and is principal investigator in most SIS-related evaluations, is a registered psychologist[19].

Because LogicalOutcomes does not have a secure physical facility and does not control the computers of our consultants, we require that access to the DHIS2 and LimeSurvey

[18] Security certifications are verified at http://www.isaca.org/certification/pages/default.aspx

[19] Verification of Gillian's status as a registered psychologist: https://members.cpo.on.ca/public_register/show/819. Other relevant qualifications are credentialed evaluators (https://evaluationcanada.ca/roster-credentialed-evaluators), ISO 27001 Lead Auditors, and so on.

databases that contain personal information be through a virtual terminal located within the Knowarth facilities. See the next section.

Knowarth Technologies

Knowarth has been hosting DHIS2 for LogicalOutcomes and other non-profits for about three years. They were originally recommended by a colleague at SolutionAnalysts when Knowarth was just a small startup company. Knowarth was recognized by CIOReview as one of the 20 most promising IT startups in 2016[20], and is positively reviewed by users and employers in several online review sites[21].

According to Chintan Mehta, co-founder, and Roopang Mody, Delivery Head of Cloud and DevOps, Knowarth Technologies is secured with biometrics devices and every employee must be fingerprinted upon entry. No-one except Knowarth staff may enter the premises, and employee entries are tracked and audited to ensure they do not enter the building outside the times they are scheduled. No-one is allowed to work beyond their shift hours unless they are specifically approved, generally as a result of a Priority-1 issue within the Infrastructure team.

Backups and database maintenance are carried out automatically, and very seldom require human intervention or access into the databases. Any such access would be audited on a two-week schedule.

The DHIS2 and LimeSurvey databases, although hosted on AWS servers in Canada, are not accessible to users outside Knowarth's physical facilities in Ahmedabad, India. In other words, no-one will be able to log on from home. We are currently planning regular penetration testing and designing an independent auditing procedure that would be carried out by our own Data Protection Officer.

SIS organizations

Organizations that subscribe to SIS have access to sensitive information from respondents in the form of open-ended comments, aggregate information that could be stigmatizing to groups (such as a high percentage of youth clients with criminal records), and contact information used to send out online surveys.

LogicalOutcomes will provide links to training on research ethics and confidentiality, and control access to Power BI reports to users who have been assigned by their organizations. If organizations wish further assistance with managing confidential information we are

[20] See https://it-services.cioreview.com/vendor/2016/knowarth_technologies

[21] And regarding the existence of Knowarth's physical facilities, Gillian verified their location on Google Maps and through a number of photographs on social media showing a building with a prominent Knowarth sign and a security guard in front, along with other photos of Knowarth staff within the facility.

available on a consulting basis. Or, organizations may wish to hire their own research consultants who can help them work with SIS evaluations.

The security procedures, outlined

This section outlines the procedures that protect the integrity, availability and privacy of LogicalOutcomes information within the Office 365 environment. The specific detailed instructions and checklists are described in separate documents. The procedures in this section do not include hosting and maintenance of the DHIS2 and LimeSurvey databases, which are covered in the appendix *Hosting security processes*.

We will be testing the procedures over the next few months and making refinements based on feedback from consultants and advisors. Current versions will be available from LogicalOutcomes on request.

Since LogicalOutcomes is a project-based organization, our procedures assume that all activities happen within projects, including internal activities like Board and HR management.

1. Define roles for each project (responsibility of Executive Director and Project Manager)

There are three sets of roles.

Administration: The Executive Director, Security Officer and Data Protection Officer are responsible for respectively approving, implementing and auditing these procedures throughout the organization, with input from the Ethics and Privacy Committee of the Board. An administrative assistant helps Project Managers set up Teams and SharePoint libraries.

Project management: Each project, including internal projects, is assigned a Project Manager who is responsible for setting up the Team and folders. Most projects also have a Project Sponsor, who is the equivalent of a Principal Investigator or Owner and who ensures that the project is meeting its goals and the needs of its users.

Team members: All team members, including volunteers and students, are expected to adhere to their signed agreement regarding confidentiality and information management for LogicalOutcomes projects.

2. Set up project teams (responsibility of Project Manager)

a. Assess privacy risk and label projects and folders

- □ Fill out the Privacy Risk Assessment form[22]..
- □ In consultation with the client organization, assign the project's correct confidentiality level within the Project Charter (Open Access or Internal or Confidential-Organization).
- □ Identify any Confidential-Organization or Confidential-GDPR materials that must be managed within the project.
- □ Based on the assessment, set up Teams and project folders as described below, or assign an administrative assistant to do so.
- □ Save the Privacy Risk Assessment in the Team SharePoint library.

b. . For Internal Teams (default)

- □ Create a private Microsoft Team with the Project Manager as owner. The Project Manager may assign others as owners. Bots or apps outside Office 365 must be approved by the Project Manager before being added to the Team.
- □ Label SharePoint document folders as Confidential-Organization if required (default label is Internal).
- □ Allow the use of external information services for the work of the Team (e.g., Zoho Desk, WordPress, GitHub) but ensure that no confidential information is used in those services.

c. For Open Access Teams

- □ Create a public Microsoft Team that is open to all users with LogicalOutcomes accounts. Any LogicalOutcomes user may invite a guest user to a public Team.
- □ Invite guest users to the Team.
- □ Allow the use of external applications and services (GitHub etc.)

[22] Our privacy risk assessment is adapted from https://digital.nhs.uk/article/8489/Health-and-social-care-data-risk-model-, which may be reused for internal use but not shared publicly.

d. For Confidential Teams

- □ Create a private Microsoft Team with one owner, the Project Manager. All members must be approved and added by the Project Manager or, if unavailable, the Executive Director or Project Sponsor. The client organization will be invited to review the team member bios, and to approve new additions to the Team.
- □ Verify that all team members with access to Confidential information are appropriately trained and qualified.
- □ Require multi-factor authentication on any account accessing Confidential information (in the administration settings).
- □ Create at least one folder in the Team SharePoint library as Confidential-Organization. (enhanced encryption and access permissions will be applied automatically).
- □ Set up the SharePoint library attached to the Team. The project may need multiple protected folders with different people accessing them. If required, folders may also be protected by Cryptomator vaults, but this removes files from Office 365 indexing and makes the information less accessible to team members.
- □ If a team member needs access to DHIS2 or LimeSurvey databases with personal information, request the Executive Director or Security Officer to set them up with a user account to a virtual workspace.
- □ If passwords to Confidential information must be shared (e.g., for encrypted SharePoint lists and Cryptomator vaults), share them through LastPass without revealing their content.

3. Set up policies for project information (responsibility of Security Officer)

Create protection policies for each label using SharePoint access permissions, Cryptomator and LastPass, and document them for Project Managers. Set default label as ‘Internal’.

- □ Set policies for contractor/volunteer training and qualifications for access to Confidential information.
- □ Set policies for Confidential-Organization folders and SharePoint libraries with Office 365 access restrictions, including multi-factor authentication.
- □ Set policies for Confidential-GDPR folders with Cryptomator vaults.
- □ Set policies for sensitive SharePoint list fields with client-managed encryption.
- □ Set policies for management of shared passwords through LastPass.
- □ Set policies for the adoption of any new online services that handle Confidential information (other than the existing approved services described in this paper: Office

365, LastPass, Cryptomator, and the Canadian-hosted AWS hosting of DHIS2 and LimeSurvey).

4. Wrap up projects (responsibility of Project Manager)

- □ Identify final versions of project deliverables and label them as Records for archiving within SharePoint.
- □ Delete any information that external organizations have requested be deleted at the end of the project, and ask team members to do so also.
- □ Remove access permissions from any Confidential information that has been protected by Office 365 enhanced encryption, and change the passwords of Cryptomator vaults.
- □ Tidy up the OneNote Notebook and documents within the Team SharePoint document library. If appropriate, copy documents to another Team.
- □ Encourage the dissemination of open access materials:
  - □ Ask team members to nominate anything they want to share or reuse themselves in the future.
  - □ Get written permission from client organization or external co-owners to share open access material, removing identifying information or non-LogicalOutcomes contributions if appropriate.
  - □ Zip up the material and post on Zenodo.org, listing all the contributors, both internal and external.
  - □ Share the Zenodo DOI with all team members and if appropriate in blog postings.
- □ Request the ‘Archiving Administrator’ to remove all members from the Team, including the Project Manager, and archive the Team documents (requires an E3 or E5 license).

5. Obtain contractor and volunteer agreements (responsibility of Project Manager)

- □ Ensure that each LogicalOutcomes contractor or volunteer has signed a confidentiality agreement.
- □ Ensure that each LogicalOutcomes contractor or volunteer has signed an agreement to manage LogicalOutcomes information correctly, i.e., saving project information in the

correct locations, not copying it without permission, and managing their devices and passwords responsibly.[23]

6. Manage incidents (responsibility of Project Manager and Executive Director)

- □ Document incidents according to the incident management policy (in development]
- □ Escalate to the Executive Director and Board

7. Audit and report (Responsibility of Data Protection Officer)

- □ Every three months, audit all Confidential projects to ensure they have been set up according to the procedures above.
- □ Every year, audit three Internal projects, selected according to the test plan (in development).
- □ Enter findings into Compliance Manager, including recommendations, and assign to the Executive Director for action.
- □ Escalate serious incidents to the Executive Director, Security Officer and Chair of Ethics and Privacy Committee (who is a Director of the Board).

8. Respond to security issues (responsibility of Executive Director and Board President)

- □ Respond in writing to issues raised in incident or audit reports.
- □ Make continuous improvements in security procedures.

Conclusion and disclaimer

This paper captures a moment in time in the development of LogicalOutcomes security processes. As we expand SIS, incorporating feedback from users, developers, advisors and security experts, they will certainly change. No security system is perfect, and it must be continuously modified to protect against new threats. You can get updated policies and procedures directly from LogicalOutcomes, email info@logicaloutcomes.net, with the exception of technical details that

[23] Our checklist, which will change as security practices change is based partly on the Cyber Aware initiative of the UK government. See https://www.theguardian.com/cyber-aware/2018/feb/28/no-excuses-how-to-tighten-up-your-online-security-in-10-minutes. The core advice is to install the latest software updates and use a strong, separate password for sensitive information.

would expose data to risk if we shared them. Additional GDPR guidance and tools will also be released over the next few years as organizations figure out how to deliver compliant information systems.

What we do want to maintain is a commitment to the three sets of principles – usability, responsible digital development, and accountability to users for their personal information.

Finally, by involving other nonprofits and security analysts in designing and testing our procedures, and then sharing them with the community, we hope to contribute to more effective privacy protections for the vulnerable people we all serve.

Key references and resources

Most of the references cited in this paper are listed within footnotes, and almost all of them are linked to worthy articles. This section contains only the key resources that readers might need to implement security protections.

On the definition of terms

This paper uses many technical terms, including privacy, security, integrity, availability, policies, procedures, processes, GDPR and so on. As in the field of evaluation, vocabulary in the security field is inconsistent, and everyone has different definitions depending on context.

For example, sometimes 'policy' is used to refer to overall organizational policies set by a Board of Directors, sometimes it refers to documents required for compliance purposes (like a web site's privacy policy), and sometimes it refers to fine-grained detailed procedures (like Office 365 encryption policies applied to the Confidential label).

We have tried to make the terms clear in the context of the paper. If readers wish formal definitions of privacy and security terms, we suggest that you begin with the definitions provided within the General Data Protection Regulation (GDPR) (see the next section). For a general overview, the Wikipedia article on information security is good.[24]

General Data Protection Regulation (GDPR)

There are massive amounts of online resources regarding the GDPR. We suggest starting with the UK's Information Commissioner's Office at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The UK National Health Service has recently released guidance on criteria for cloud hosting of highly sensitive personal health information, posted at https://digital.nhs.uk/Offshoring-and-

[24] See https://en.wikipedia.org/wiki/Information_security

the-use-of-public-cloud-services. We relied heavily on those documents in designing our hosting service. They are:

- The health and social care cloud security good practice guide.
- The health and social care cloud risk framework.
- The health and social care data risk model.
- The health and social care cloud security - one page overview.

Our other major resource was Microsoft's Compliance Manager for Office 365 GDPR, available at https://servicetrust.microsoft.com/. The Compliance Manager is a free service for Office 365 subscribers.

LogicalOutcomes security policies

Information security and data protection policy (being revised – the current version is at http://logicaloutcomes.net/wp-content/uploads/2017/10/Information-Security-Policy-LogicalOutcomes-2017-10-02.pdf)

Privacy policy: The LogicalOutcomes privacy policy has been revised to comply with GDPR requirements. It's long because it addresses all the issues that are required by GDPR.

Training on research ethics and confidentiality

We are still refining our training qualifications for Confidential projects, and they will be included in the upcoming Human Resources policy.

In general, we prefer contractors and volunteers who have been qualified through an external certification or training course that covers research ethics and/or confidentiality. Examples include a CES Credentialed Evaluator[25], a registered psychologist, or a security certification through ISACA[26].

For team members accessing Confidential information who are not independently qualified, we require that they take relevant training. We are reviewing the following free courses with an aim to making specific recommendations of courses for specific project functions.

The Canadian Tri-Council training for research involving human subjects

TCPS2: CORE (Course on Research Ethics): A three-hour course that covers ethical protocol for researchers working with human subjects. Designed for academic researchers in the social sciences, but relevant to evaluators.

[25] https://evaluationcanada.ca/ce
[26] http://www.isaca.org/CERTIFICATION

Research ethics online training by the Global Health Training Center

These materials target medical researchers primarily, but much of their content is useful to evaluators.

Research ethics online training: A modular certificate course that takes about seven hours to complete.

Short courses: Courses lasting 30-60 minutes, which provide guidance on issues like informed consent, responsible data management, and other topics relevant to evaluators.

General Data Protection Regulation

The UK has adopted GDPR even though they are leaving the European Union, and they offer some great training resources to help organizations implement it.

Information Commissioner's Office, Resources and Support: A training platform aimed at organizations, featuring checklists, toolkits, webinars, videos and other training resources.

Appendices

The asset and risk register[27]

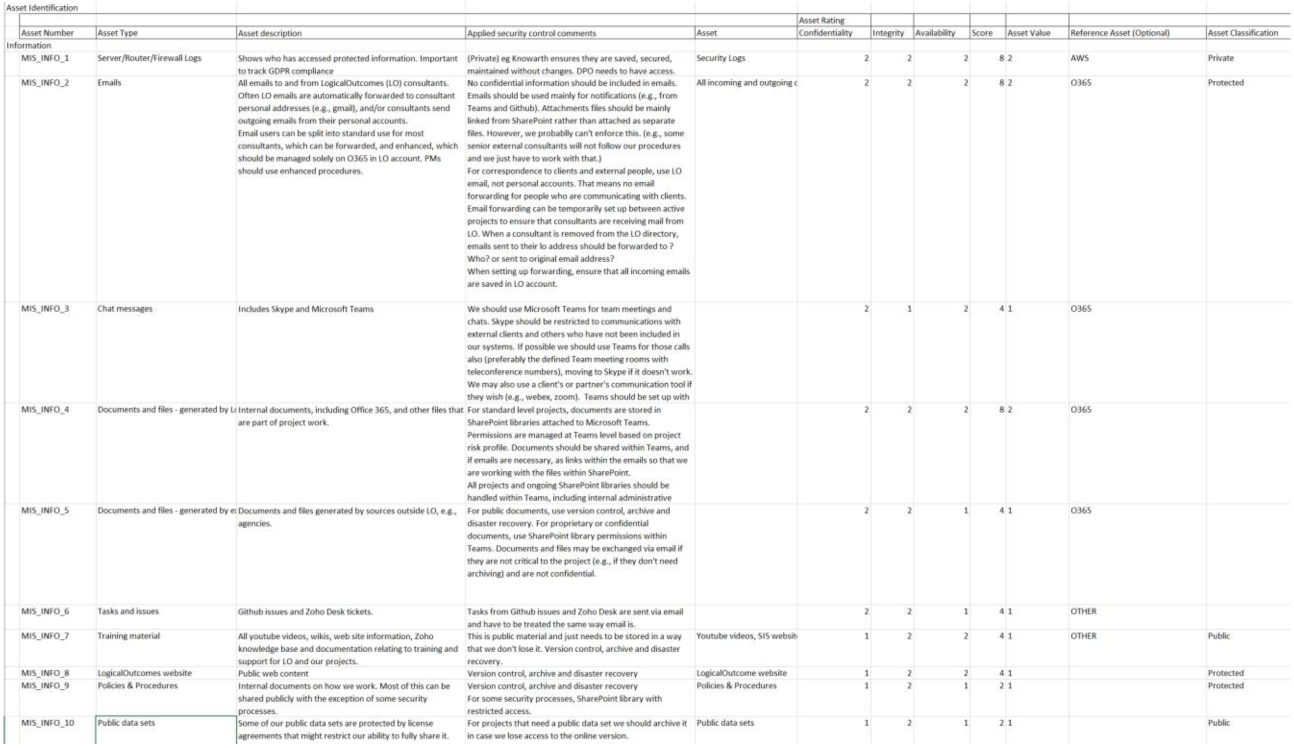
For readers who want to dig into the gruesome details of the asset and risk register, we have excerpted key parts of the process below. These are mainly drafts that we used during the development process, and there have been changes since.

Guidelines for filling asset register	
Exclusions: Consumable items, e.g., stationary items, computer accessories	
Asset #	Give a unique number to every identified asset according to the following convention: Dep-Info-ID, where: Dep is the first 3 letters of department/project name or the Excel worksheet name Info is the first 4 letters of Asset Category: 1. Info - Information. 2 Papr - Paper, 3. Hdwp - Hardware - Physical, 4. Stfw - Software, 5. Pepl - People (designation), 6. Etxs - Extension service, 7. Copi - Company image (reputation or goodwill) ID is the unique number starting from 1,2,3
Asset Type	Specify the most appropriate asset type (information, service, software, hardware, paper, people)
Asset	Specify the name and description of asset
Asset Rating	**Confidentiality**: Refers to safeguarding the secrecy of the organization's information. H - 3 - High confidential, severe problem if disclosed to external parties. For details refer to Data Classification and Control Policy M - 2 - Medium restricted, should not be shared with unauthorized parties, minor problem if disclosed L - 1 - No or Low problem - negligible impact and small affect on organization or other entities
	Integrity: Refers to safeguarding the accuracy and completeness of information and processing methods. H - 3 - Business critical that information is accurate and of high quality M - 2 - Medium problem if information is inaccurate or low quality, some errors are acceptable L - 1 - No significant problem if information is inaccurate or incomplete (i.e., the effort to protect this level is less than the effort to live without it)

[27] The guidelines for the risk and asset register were provided by Moiz Azam.

	Availability: Refers to ensuring that authorized users have access to information and associated assets when required. H - 3 - High mission critical, lack of availability can have a severe impact on business processes if outage lasts more than an hour during business hours M - 2 - Medium severity of problem if asset is available; a short outage of a few hours is tolerable L - 1 - Low severity - an extended outage is tolerable
	Score: Score is the sum of above mentioned three values, i.e., Confidentiality, Integrity and Availability
Asset Value	Indication of asset importance
Asset Owner	Provide the name of the person or role who is responsible for allowing access to the asset
Asset Location	Specify the actual physical location of asset, in enough detail so that someone could locate it, or the online location.
Reference Asset	Specify other assets that are dependent uon this asset, or on which this asset depends. Password safe?
Asset Classification	Select the appropriate asset label from the list according to the Information Classification Procedure, using followoing labels: 0**. Public:** Compromise of information would not damage the organization and other entities; i.e., general public may be granted access **1. Internal:** Compromise of information might embarrass the organization or other entities (e.g, releasing the names of agency staff without their permission, or sharing proprietary documents that do not contain PHI without permission) **2. Private**: Compromise of information could cause limited damage to the organization and other entities (e.g., sensitive Human Resources information about consultants) **3. Protected**: Compromise of information would damage the reputation of the organization and possibly harm other entities (e.g., sensitive Personal Health Information)

Excerpt of asset register



Asset Identification											
					Asset Rating						
Asset Number	Asset Type	Asset description	Applied security control comments	Asset	Confidentiality	Integrity	Availability	Score	Asset Value	Reference Asset (Optional)	Asset Classification
Information											
MIS_INFO_1	Server/Router/Firewall Logs	Shows who has accessed protected information. Important to track GDPR compliance	(Private) eg Knowarth ensures they are saved, secured, maintained without changes. DPO needs to have access.	Security Logs	2	2	2	8	2	AWS	Private
MIS_INFO_2	Emails	All emails to and from LogicalOutcomes (LO) consultants. Often LO emails are automatically forwarded to consultant personal addresses (e.g., gmail), and/or consultants send outgoing emails from their personal accounts. Email users can be split into standard use for most consultants, which can be forwarded, and enhanced, which should be managed solely on O365 in LO account. PMs should use enhanced procedures.	No confidential information should be included in emails. Emails should be used mainly for notifications (e.g., from Teams and Github). Attachments files should be mainly linked from SharePoint rather than attached as separate files. However, we probablly can't enforce this. (e.g., some senior external consultants will not follow our procedures and we just have to work with that.) For correspondence to clients and external people, use LO email, not personal accounts. That means no email forwarding for people who are communicating with clients. Email forwarding can be temporarily set up between active projects to ensure that consultants are receiving mail from LO. When a consultant is removed from the LO directory, emails sent to their lo address should be forwarded to ? Who? or sent to original email address? When setting up forwarding, ensure that all incoming emails are saved in LO account.	All incoming and outgoing c	2	2	2	8	2	O365	Protected
MIS_INFO_3	Chat messages	Includes Skype and Microsoft Teams	We should use Microsoft Teams for team meetings and chats. Skype should be restricted to communications with external clients and others who have not been included in our systems. If possible we should use Teams for those calls also (preferably the defined Team meeting rooms with teleconference numbers), moving to Skype if it doesn't work. We may also use a client's or partner's communication tool if they wish (e.g., webex, zoom). Teams should be set up with		2	1	2	4	1	O365	
MIS_INFO_4	Documents and files - generated by L	Internal documents, including Office 365, and other files that are part of project work.	For standard level projects, documents are stored in SharePoint libraries attached to Microsoft Teams. Permissions are managed at Teams level based on project risk profile. Documents should be shared within Teams, and if emails are necessary, as links within the emails so that we are working with the files within SharePoint. All projects and ongoing SharePoint libraries should be handled within Teams, including internal administrative		2	2	2	8	2	O365	
MIS_INFO_5	Documents and files - generated by e	Documents and files generated by sources outside LO, e.g., agencies.	For public documents, use version control, archive and disaster recovery. For proprietary or confidential documents, use SharePoint library permissions within Teams. Documents and files may be exchanged via email if they are not critical to the project (e.g., if they don't need archiving) and are not confidential.		2	2	1	4	1	O365	
MIS_INFO_6	Tasks and issues	Github issues and Zoho Desk tickets.	Tasks from Github issues and Zoho Desk are sent via email and have to be treated the same way email is.		2	2	1	4	1	OTHER	
MIS_INFO_7	Training material	All youtube videos, wikis, web site information, Zoho knowledge base and documentation relating to training and support for LO and our projects.	This is public material and just needs to be stored in a way that we don't lose it. Version control, archive and disaster recovery.	Youtube videos, SIS websit	1	2	2	4	1	OTHER	Public
MIS_INFO_8	LogicalOutcomes website	Public web content	Version control, archive and disaster recovery	LogicalOutcome website	1	2	2	4	1		Protected
MIS_INFO_9	Policies & Procedures	Internal documents on how we work. Most of this can be shared publicly with the exception of some security processes.	Version control, archive and disaster recovery For some security processes, SharePoint library with restricted access.	Policies & Procedures	1	2	1	2	1		Protected
MIS_INFO_10	Public data sets	Some of our public data sets are protected by license agreements that might restrict our ability to fully share it.	For projects that need a public data set we should archive it in case we lose access to the online version.	Public data sets	1	2	1	2	1		Public

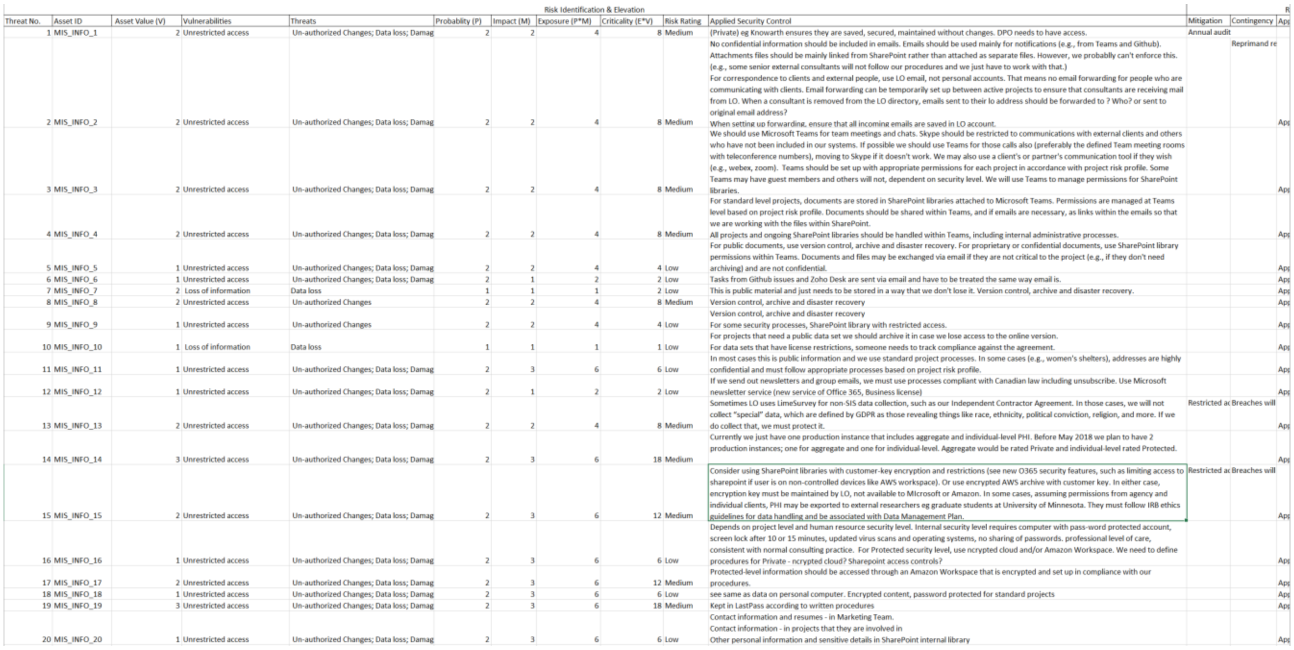
Guidelines for documenting risk management workbook

Threat No.	Assign threat number in series starting from 1 2 3
Asset No.	Asset Number should be the same as in the Asset Register. it should be copied from the Asset Register
Asset Value (V)	Asset Value should be copied from the Asset Register, against the respective asset
Threat / Vulnerability	Threat is basically the potential cause of an unwanted impact to a system or organization.
Probability (P)	Probability is chances of risk occurrence. On The basis of below mentioned criteria you can rate the probability:
	High - 3 - Threat has high probability of occurrence;
	Medium - 2 - foreseeable probability of occurrence; and
	Low - 1 - Low probability of occurrence.
Impact (M)	The expected harm (loss) of a risk is Impact that means if Impact compromised, how severely it can damage the company's business:

	Serious - 3 - Significant expenditure of resources required or damage to reputation and confidence
	Significant - 2 - Tangible harm. extra effort required to repair
	Minor - 1 - No extra effort required to repair
Exposure (E=P*M)	Auto Calculated formula describing how severely a risk can damage the business (Probability * Impact)
Risk Criticality (E*V)	Auto calculated Formulas (Exposure * Asset Value), describing how critical is for business to manage this risk
Risk Rating	Auto calculated formula describing that whether a risk is high or medium or low depending upon the criticality, exposure, impact and probability of a threat.
	There is a formula in place to show you the rating of Risk (High, Medium, or Low).
	Formula = IF Critically < 7 then Risk Rating a Low, Else IF Criticality < 19 then Risk Rating is Medium, else Risk Rating is High .
	Risk **Rating Range is :** 1 - 6 a Low. 7-18 a Medium, and 19 - 27 a High
Applied Security Control	Describe current controls which are in place or which are being used to mitigate the respective threat. Controls can be physical or logical.
Risk Treatment Methodology	**Mitigation**: Write one or more approaches to control, avoid, minimize. or otherwise mitigate the risk. Mitigation approaches may reduce the probability or the impact.
	Contingency: Write the actions that will be taken to deal with the situation if this risk factor actually becomes a problem.
	Appropriate Management Action: Write the appropriate action that the management has recommended. Committed: means that the management has committed, will be done as and when the project will execute Approved: means that the management has approved, and has to be executed immediately Disapproved: means that the management has disapproved, and does not need any action
	Resources: Mention all kind of resources that might be needed to reduce the risk. The resources might be human, machine, training. investment etc.
	Priority: Prioritize which risk requires treatment first on the basis of below mentioned criteria. Rate the priority: High: Should be executed immediately Medium: Should be scheduled and executed Low: Can be executed as per need

Risk Owner	Write the name of the person who is responsible for the management and mitigation or contingency of respective risk

Excerpt of risk management workbook



							Risk Identification & Elevation						R
Threat No.	Asset ID	Asset Value (V)	Vulnerabilities	Threats	Probablity (P)	Impact (M)	Exposure (P*M)	Criticality (E*V)	Risk Rating	Applied Security Control	Mitigation	Contingency	App
1	MIS_INFO_1	2	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	2	4	8	Medium	(Private) eg Knowarth ensures they are saved, secured, maintained without changes. DPO needs to have access.	Annual audit		
2	MIS_INFO_2	2	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	2	4	8	Medium	No confidential information should be included in emails. Emails should be used mainly for notifications (e.g., from Teams and Github). Attachments files should be mainly linked from SharePoint rather than attached as separate files. However, we probablly can't enforce this. (e.g., some senior external consultants will not follow our procedures and we just have to work with that.) For correspondence to clients and external people, use LO email, not personal accounts. That means no email forwarding for people who are communicating with clients. Email forwarding can be temporarily set up between active projects to ensure that consultants are receiving mail from LO. When a consultant is removed from the LO directory, emails sent to their lo address should be forwarded to ? Who? or sent to original email address? When setting up forwarding, ensure that all incoming emails are saved in LO account.		Reprimand re	App
3	MIS_INFO_3	2	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	2	4	8	Medium	We should use Microsoft Teams for team meetings and chats. Skype should be restricted to communications with external clients and others who have not been included in our systems. If possible we should use Teams for those calls also (preferably the defined Team meeting rooms with teleconference numbers), moving to Skype if it doesn't work. We may also use a client's or partner's communication tool if they wish (e.g., webex, zoom). Teams should be set up with appropriate permissions for each project in accordance with project risk profile. Some Teams may have guest members and others will not, dependent on security level. We will use Teams to manage permissions for SharePoint libraries.			App
4	MIS_INFO_4	2	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	2	4	8	Medium	For standard level projects, documents are stored in SharePoint libraries attached to Microsoft Teams. Permissions are managed at Teams level based on project risk profile. Documents should be shared within Teams, and if emails are necessary, as links within the emails so that we are working with the files within SharePoint. All projects and ongoing SharePoint libraries should be handled within Teams, including internal administrative processes.			App
5	MIS_INFO_5	1	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	2	4	4	Low	For public documents, use version control, archive and disaster recovery. For proprietary or confidential documents, use SharePoint library permissions within Teams. Documents and files may be exchanged via email if they are not critical to the project (e.g., if they don't need archiving) and are not confidential.			App
6	MIS_INFO_6	1	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	1	2	2	Low	Tasks from Github issues and Zoho Desk are sent via email and have to be treated the same way email is.			App
7	MIS_INFO_7	2	Loss of information	Data loss	1	1	1	2	Low	This is public material and just needs to be stored in a way that we don't lose it. Version control, archive and disaster recovery.			App
8	MIS_INFO_8	2	Unrestricted access	Un-authorized Changes	2	2	4	8	Medium	Version control, archive and disaster recovery			App
9	MIS_INFO_9	1	Unrestricted access	Un-authorized Changes	2	2	4	4	Low	Version control, archive and disaster recovery For some security processes, SharePoint library with restricted access.			App
10	MIS_INFO_10	1	Loss of information	Data loss	1	1	1	1	Low	For projects that need a public data set we should archive it in case we lose access to the online version. For data sets that have license restrictions, someone needs to track compliance against the agreement.			App
11	MIS_INFO_11	1	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	3	6	6	Low	In most cases this is public information and we use standard project processes. In some cases (e.g., women's shelters), addresses are highly confidential and must follow appropriate processes based on project risk profile.			App
12	MIS_INFO_12	1	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	1	2	2	Low	If we send out newsletters and group emails, we must use processes compliant with Canadian law including unsubscribe. Use Microsoft newsletter service (new service of Office 365, Business license)			App
13	MIS_INFO_13	2	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	2	4	8	Medium	Sometimes LO uses LimeSurvey for non-SIS data collection, such as our Independent Contractor Agreement. In those cases, we will not collect "special" data, which are defined by GDPR as those revealing things like race, ethnicity, political conviction, religion, and more. If we do collect that, we must protect it.	Restricted ac	Breaches will	App
14	MIS_INFO_14	3	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	3	6	18	Medium	Currently we just have one production instance that includes aggregate and individual-level PHI. Before May 2018 we plan to have 2 production instances; one for aggregate and one for individual-level. Aggregate would be rated Private and individual-level rated Protected.			App
15	MIS_INFO_15	2	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	3	6	12	Medium	Consider using SharePoint libraries with customer-key encryption and restrictions (see new O365 security features, such as limiting access to sharepoint if user is on non-controlled devices like AWS workspace). Or use encrypted AWS archive with customer key. In either case, encryption key must be maintained by LO, not available to MIcrosoft or Amazon. In some cases, assuming permissions from agency and individual clients, PHI may be exported to external researchers eg graduate students at University of Minnesota. They must follow IRB ethics guidelines for data handling and be associated with Data Management Plan.	Restricted ac	Breaches will	App
16	MIS_INFO_16	1	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	3	6	6	Low	Depends on project level and human resource security level. Internal security level requires computer with pass-word protected account, screen lock after 10 or 15 minutes, updated virus scans and operating systems, no sharing of passwords. professional level of care, consistent with normal consulting practice. For Protected security level, use ncrypted cloud and/or Amazon Workspace. We need to define procedures for Private - ncrypted cloud? Sharepoint access controls?			App
17	MIS_INFO_17	2	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	3	6	12	Medium	Protected-level information should be accessed through an Amazon Workspace that is encrypted and set up in compliance with our procedures.			App
18	MIS_INFO_18	1	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	3	6	6	Low	see same as data on personal computer. Encrypted content, password protected for standard projects			App
19	MIS_INFO_19	3	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	3	6	18	Medium	Kept in LastPass according to written procedures			App
20	MIS_INFO_20	1	Unrestricted access	Un-authorized Changes; Data loss; Damag	2	3	6	6	Low	Contact information and resumes - in Marketing Team. Contact information - in projects that they are involved in Other personal information and sensitive details in SharePoint internal library			App

Summary of assets by security level

The following table is a working document that shows how we ended up categorizing our various information assets by the level of risk they represent, along with notes on possible procedures. They are not in final form, and we've made several changes since the table was created.

Information asset by level of security access	3 -Confidential - GDPR	2 - Confidential - Organization	1 - Internal	0 - Open access
Public - for anyone • LogicalOutcomes web site • Training materials • Public Github repos • Public datasets • External non-confidential documents, files • Power BI public dashboards • Zenodo documents	NA	NA	Creation of content belongs under 'internal' access	Version control, archive, offsite disaster recovery applies to everything
Internal - for consultants or	NA	Decisions on who	We should have a	NA

Information asset by level of security access	3 -Confidential - GDPR	2 - Confidential - Organization	1 - Internal	0 - Open access
volunteers who have signed confidentiality agreements and have professional practices for handling business information • Email • Most Teams, SharePoint libraries and sites • Private Github repos and issues • Passwords and access for content creation of public materials (e.g, DHIS2 curriculum, LO web site) • Skype chats • Zoho Desk tickets • Contact information for agencies, contractors, associates • Desktop computer files • Board meetings, agreements • DHIS2 demo and training instance(s) • LimeSurvey development, showcase surveys, reference surveys, training • SharePoint development, demo, training • Project contracts and statements of work • Power BI reporting dev space • DHIS2 development instance		has access to these resources (adding users and assigning permission levels for projects)	resume or bio to show that they are a reasonable choice to access our systems (e.g., in our HR list), including volunteers. Doesn't have to be that formal.	
Confidential - Organization - for specified people with enhanced security processes • Adding users and assigning permission levels (not for Protected resources) • Passwords for LO resources (not Protected) • Specified Teams and SharePoint libraries and sites: Projects with higher security requirements • DHIS2 production reports	NA	For agencies who use SIS, assign individual permissions at each agency to Power BI reports Use O365 protections e.g., for SharePoint files we can limit access. E5 licenses for		NA

Information asset by level of security access	3 -Confidential - GDPR	2 - Confidential - Organization	1 - Internal	0 - Open access
and dashboards with aggregate or anonymous qualitative information, including for agency clients		enhanced security options in Office 365. Private teams, DLP protection and encryption		
Confidential - GDPR - for specified screened and certified people with enhanced security processes ● DHIS2 production individual-level information ● LimeSurvey production instance ● Archived PHI from DHIS2 ● Desktop files with PHI information (e.g., for data mining)	Must use virtual desktop for access, managed within Knowarth facilities. Permission levels tightly controlled and access logged. All sensitive info has client-controlled encryption key. Sharepoint lists with email addresses encrypted. Crytomator to store analytic files in vaults in closed-down SharePoint site (no access except from AWS workspace). Analyst can save reports without confidential info into another SharePoint library owned by the agency. Customer managed key for encryption, and multifactor authentication. Signed authorization by agencies, with appropriate consent forms, for access by other analysts using the virtual workspaces.	NA	NA	NA

SIS privacy risk assessment

We used the risk framework published by the UK National Health Service in their guidance on cloud hosting of personal health information[28]. Following is an excerpt of the SIS privacy assessment. Note that for our own purposes we have not rewritten it to refer to specific Canadian laws; it's good enough 'as is' to assess privacy risks for all the kinds of personal data that health analysts may work with.

At the moment, SIS does not contain the highest risk data described below. However, we are building a system that can host it when we do start collecting high risk data.

Data Type	***Applicable? (Yes/No)***	***Description***
Publicly available information	Yes	Statistical material that is intended for public distribution. Identification from these materials, with or without any other materials, is not feasible. *If this is the **only** data being processed, move straight to scale and persistency categories.*
Synthetic (test) data	Yes	Synthetic (test) data is fictional data, engineered to be representative of real data, that is created in order to avoid the need to use real data when developing and testing IT systems. Synthetic data must pose zero risk of contributing to the revealing of any personal data.
Aggregate data	Yes	Summarised and anonymised data, but which is not suitable for public distribution, due to the risk that it may be used with other material to contribute to the re-identification of individuals. The risk of such re-identification is not significant, but does exist (especially in the presence of a sustained and skilled attack).
Already encrypted materials	No	Materials that are already encrypted before they touch the cloud, using strong cryptography as defined by the current version of NIST SP800-57 and where the encryption keys are not stored with the cloud provider.
PID Personal data - Demographic	Yes	Information about the individual rather than their clinical details
PID Personal Data - High Risk Demographic	No	Demographic data where, in the event of a breach, there is a high risk of significant harm
Personal Confidential Data (PCD)	Yes	PCD is based on the ICO definition of sensitive personal data (that includes clinical information), extended within health and social care to include:- • deceased persons • information that is given in confidence and is owed a duty of care, such as: o Social care records / child protection / housing assessments o DNA / finger prints o Bank / financial / credit card details o National Insurance number / Tax, benefit or pension records o Travel details (for example at immigration control, or Oyster records) o Passport number / information on immigration status / travel records o Work record or place of work / School attendance / records
PCD - Legally-restricted	No	Sensitive personal data that are subject to additional regulations or statute.

[28] The Excel risk model is at https://digital.nhs.uk/Health-and-social-care-data-risk-model and the instructions are at https://digital.nhs.uk/article/8488/Health-and-social-care-cloud-risk-framework. The risk model may be used internally by organizations but not published without permission.

PCD - Extra-delicate	Yes	Sensitive personal data that are sometimes seen to be additionally delicate, but for which there are no legal restrictions. This determination is often not consistent, but is commonly-held, and is often related to conditions that attract, or are considered to attract, stigma. For example, HIV status, mental health conditions, other conditions contained within the SCR “sensitive code” list. Whilst many patients see information on these kinds of condition to be particularly private and not to be shared under any circumstances, others see them as important to share, and for any stigmas to be removed.
Anonymised data	Yes	Sensitive personal data that has been subject to de-identification and/or other privacy-enhancing techniques, in line with the ICO Anonymisation Code of Practice. Risk of re-identification is remote (and would be based on activities that are illegal and/or break contractual arrangements). No way of authorised linking with other data-sets.
Reversibly-pseudonymised data	No	Pseudonymised data where the pseudonym is also intended to be used to facilitate re-identification where that is supported by business purpose and legal basis.
Irreversibly-pseudonymised data	Yes	Pseudonymised data where re-identification is not intended.
Patient account data	No	Account credentials (including any recovery materials) for citizen accounts for patient-facing online health tools
Patient choices	Yes	Statements / preferences made by citizens regarding the use of their data
Patient meta-data (identifiable)	No	Information about how identified patients have used patient-facing online health tools
Patient meta-data (linkable)	Yes	Information about how patients have used patient-facing online health tools (not identified, but linkable across sessions)
Professional account data	No	Account credentials (including any recovery materials) for professional user (eg clinician, health professional) accounts that control access to any personal data (including PCD)
Professional account data (less-sensitive)	Yes	Account credentials (including any recovery materials) for professional user (eg clinician, health professional) accounts that control access to anonymised information
Audit: professional User meta-data	Yes	Information about how users have used clinical or administrative tools that process personal data
Audit: personal data	No	Data describing the use of a clinical or administrative system that processes personal data, where that audit data itself includes or references PCD
Audit: non-personal data	Yes	Data describing the use of a clinical or administrative system, where that audit data itself does not include or reference PCD
Key materials: very short-lived	No	One-time decryption keys
Key materials: rotatable	No	Material that provide linkage between reversibly-pseudonymised data and personal data, that persists over time and over user sessions but is generally rotatable
Key materials: long-lived	Yes	Material that provide long-lived and persistent linkage between reversibly-pseudonymised data and personal data, or provides a significant security function

SIS hosting security processes

The following table is a living document that we are using to define our hosting procedures. It's in development. We have adapted the UK National Health Services 'Guidance on cloud hosting for personal health information' NHS 2018[29]. We are comparing SIS hosting to the level of security that NHS recommends for off-shore cloud hosting of the most sensitive government health information. At this point we can't deliver every feature fully, but this table gives us something to work with in the future.

Note that many of the features are provided 'out of the box' by Amazon Web Services. Those features are described in an audit report available at https://d1.awsstatic.com/whitepapers/compliance/AWS_IT_Grundschutz_TUV_Certification_Workbook.pdf

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
1	**Data in transit protection** *User data transiting networks should be adequately protected against tampering and eavesdropping.*	TLS (Version 1.2 or above) OR IPsec or TLS VPN gateway	The Cloud Provider should:-		
			1. Utilise strong cryptography as defined by NIST SP800-57 to encrypt communications: a. Internally between Cloud Components. b. Between Cloud Data Centres. c. Between the Cloud admin portal and the Cloud.	Y	
			2. Undertake annual assessment against a recognised standard such as ISO to test the security of the communication: a. Internally between Cloud Components. b. Between Cloud Data Centres. c. Between the Cloud admin portal and the Cloud. Ensure that the assessment is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Y	AWS in all regions is certified according to ISO standards. Every year they must go through an audit.
			The Service User should:-		

[29] See https://digital.nhs.uk/article/8491/Health-and-social-care-cloud-security-good-practice-guide

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
			1. Utilise strong cryptography as defined by NIST SP800-57 to encrypt communications between the Cloud and the End-user.	Y	SSL with TLS1 encryption
			2. Undertake regular (minimum yearly) penetration testing of the communication between the Cloud and the End-user. Ensure that the Penetration test is well scoped such that 'Data in transit protection' is fully tested. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Planned	
2	**Asset protection and resilience** *User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.*				
2.1	**Physical location and legal jurisdiction** *In order to understand the legal circumstances under which your data could be accessed without your consent you must identify the locations at which it is stored, processed and managed.* *You will also need to*	Known locations for storage, processing and management	The Cloud Provider must:-		
			1. Provide cloud infrastructure (which includes all hardware, software, networks and the physical data centres that house it all) within the UK, European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield, or in Canada	Y	Done by AWS
			2. Provide independent validation that the data centres are actually physically located within the UK, European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield, or in Canada	Y	Done by AWS
			3. State the legal jurisdiction(s) to which your data is subject to.	Y	AWS Canadian servers

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
	understand how datahandling controls within the service are enforced, relative to relevant legislation.		The Service User should:-		
			1. Only use Cloud Infrastructures to store and process data that are physically located within the UK, European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield, or in Canada	Y	Done by AWS
			2. Review the Cloud Provider's T&Cs to ensure they are compliant with the General Data Protection Regulation (GDPR).	Y	AWS is compliant already.
2.2	**Data centre security** *Locations used to provide cloud services need physical protection against unauthorised access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data.*	Conforms to a recognised standard	The Cloud Provider should:-		
			1. Hold and maintain certification to ISO 27001. Prove that the scope of certification includes the physical security of the data centres. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST scheme.	Y	Done by AWS
2.3	**Data at rest protection** *To ensure data is not available to unauthorised parties with physical access to infrastructure, user data held within the service should be*	Encryption of all physical media	The Cloud Provider should:-		
			1. Provide encryption facilities to ensure that no data is written to storage in an unencrypted form.	Y	Encryption at rest will be applied to DHIS2 Quick start at beginning of May 2018.
			2. Provide secure key management service providing strong cryptography as defined by the current version of NIST and FIPS standards. e.g. NIST SP800-57 Part 1'. The service must provide detailed audit reporting on access of the keys.	Y	Done by Knowarth and AWS (confirm technical details in section 2.3.2 below)

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
	protected regardless of the storage media on which it's held. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media.		3. Confirm that the encryption utilises strong cryptography as defined by the current version of NIST SP800-57.	Y	Done by AWS
			4. Undertake annual assessment against a recognised standard such as ISO or FIPS 140-2 to test the encryption. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Y	Done by AWS
			The Service User should:-		
			1. Ensure that the encryption is appropriately configured when you implement the system on your chosen cloud provider.	Y	Knowarth and AWS
			2. Ensure keys are managed by the data controller. Keys can be stored either locally or in an HSM service provided by the cloud supplier. The key management solution should utilise strong cryptography as defined by the current version of NIST and FIPS standards. e.g. NIST SP800-57 Part 1	Planned	Done by Knowarth using volume LUKS Filesystem encryption with key controlled by Knowarth, inaccessible to AWS.
2.4	**Data sanitisation** *The process of provisioning, migrating and deprovisioning resources should not result in unauthorised access to user data.*	Explicit overwriting of storage before reallocation	The Cloud Provider should:-		
			1. Provide assertions regarding their data sanitisation approach.	Y	Done by AWS
			2. Show that the specified data sanitation approach has been validated by a suitably qualified independent third party.	Y	
2.5	**Equipment disposal** *Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the*	A recognised standard for equipment disposal is followed OR A third-party destruction service is used	The Cloud Provider should:-		
			1. Hold certification to CSA CCM v3.0 OR ISO/IEC 27001. Prove that the scope of certification validates the secure equipment disposal. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.	Y	Done by AWS

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
	service, or user data stored in the service.		The Cloud Provider should:-		
			1. Ensure the security of the equipment and prove the chain of custody until the equipment is successfully destroyed.	Y	Done by AWS
			2. Demonstrate that the third-party services have been assessed against a recognised standard, such as the CESG Assured Service (Destruction) scheme. Prove that the scope of the assessment validates the secure equipment disposal and chain of custody. Demonstrate that the assessment was performed by a suitably qualified expert party such as those certified under the CREST scheme.	Y	Done by AWS
2.6	**Physical resilience and availability** *Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on your business.*	The service provider commits to a Service Level Agreement (SLA) AND Analysis of the design	**Service Classification (See appendix B):**		
			The Cloud Provider should:-		
			1. Provide a contractual commitment to SLAs, with remedies available should the SLA be missed.	Y	Done by AWS
			2. Prove that the data centres are certified to Uptime Institute Tier 2 or equivalent qualified provider such as those certified under the CREST scheme.	Y	Done by AWS
			3. Prove that the data centres are certified to Uptime Institute Tier 3 or equivalent qualified provider such as those certified under the CREST scheme.	Y	Done by AWS
			4. Provide two or more "availability zones" / Data Centres in-line with the requirements in 2.1.	Y	Done by AWS (AWS has multiple availability zones in Canada)
			The Service User should:-		
			1. Design for failure. Solutions should be architected for cloud such that they are resilient regardless of the underlying cloud infrastructure.	Y	Daily backups in case one availability zone is down, can replicate in another availability zone. Some data loss within the same day.

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
			2. Use at least one availability zone / Data Centre.	Y	Done by AWS
			3. Have resilient network links to the zone / Data Centre.	Y	Done by AWS
			4. Use multiple availability zones / Data Centres.	Y	Done by AWS
			5. Have resilient network links to each zone / Data Centres.	Y	Done by AWS
			6. Use different cloud vendors or multiple regions from the same vendor.	Y	Done by AWS
			7. Have resilient network links to each region / vendor.	Y	Done by AWS
			8. Ensure their system has DDoS protection. This may be provided by the Cloud vendor or a third party.	Y	Apache mod_evasive module
3	**Separation between users** *A malicious or compromised user of the service should not be able to affect the service or data of another.*	Virtualisation technologies (e.g. a hypervisor) provide separation between users OR Other software provides separation between users	The Cloud Provider should:-		
			1. Provide Supplier Assertions regarding their approach to user/customer environment separation.	Y	Done by AWS
			2. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'separation between users/ customer environment'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Y	AWS controls this through identity access management, including MFA. This is audited through AWS annual audit.
			3. Hold and maintain certification to ISO27017 for the Cloud Platform. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST scheme.	Y	Done by AWS
			The Service User should:-		
			1. Undertake end-to-end Penetration testing of the solution.	Planned	

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
			2. Implement a GPG13 compliant Protective Monitoring solution.	N	Very few hosting solutions are compliant with this standard. Knowarth uses performance monitoring and log analysis tool (Motodata)
4	**Governance framework** *The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.*	Conformance with a recognised standard	The Cloud Provider should:-		
			1. Hold and maintain certification to CSA's STAR programme OR ISO/IEC 27001. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST scheme.	Y	Done by AWS
			2. Prove that the scope of certification includes the governance framework goals set out below: a. A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer'. b. A documented framework for security governance, with policies governing key aspects of information security relevant to the service. c. Security and information security are part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk. d. Processes to identify and ensure compliance with applicable legal and regulatory requirements.	Y	Done by AWS

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
5	**Operational security** *The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.*				
5.1	**Configuration and change management** *You should ensure that changes to the system have been properly tested and authorised. Changes should not unexpectedly alter security properties*	Conformance with a recognised standard	The Cloud Provider should:-		
			1. Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001. Prove that the scope of certification includes configuration and change management processes. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.	Y	Done by AWS
			The Service User should:-		
			1. Maintain an accurate inventory of the assets which make up the service, along with their configurations and dependencies.	Y	LogicalOutcomes role
			2. Ensure changes to the service are assessed for potential security impact, and the implementation of changes are managed and tracked through to completion.	Y	LogicalOutcomes role
5.	**Vulnerability**	Conformance with a	The Cloud Provider should:-		

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
2	**management** *You should identify and mitigate security issues in constituent components*	recognised standard	1. Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001, ISO/IEC 27017. Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.	Y	Done by AWS
			2. Manage vulnerabilities in a manner that aligns with ISO 30111 and show ISO / CSA compliance to validate the process.	Y	Done by AWS. Knowarth will run AWS Inspector monthly.
			3. Prove that mitigations for discovered vulnerabilities are implemented for the server-less devices, hypervisors and supporting infrastructure, within the NCSC best practice timescales set out below:- a. 'Critical' vulnerabilities should be mitigated within 24 hours b. 'Important' vulnerabilities should be mitigated within 2 weeks. c. 'Other' vulnerabilities mitigated within 8 weeks. If compensating controls are in place to reduce the vulnerability risk, the timescales can be adjusted accordingly	Y	Done by AWS
			The Service User should:-		
			1. Undertake patching or vulnerability management for the guest operating system and application components, within the NCSC best practice timescales set out below:- a. 'Critical' patches should be deployed within 24 hours b. 'Important' patches should be deployed within 2 weeks of a patch becoming available c. 'Other' patches deployed within 8 weeks of a patch becoming available	Y	

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
			Undertake regular (min yearly) penetration testing. Ensure that the Penetration test is well scoped such that 'security vulnerabilities in the Operating system and components above' are fully tested. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Planned	Details to be confirmed
5.3	**Protective monitoring** *You should put measures in place to detect attacks and unauthorised activity on the service*	Conformance with a recognised standard	The Cloud Provider should:-		
			1. Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001 and ISO/IEC 27017 Prove that the scope of certification includes protective monitoring controls showing that:- a. The service generates adequate audit events to support effective identification of suspicious activity b. These events are promptly analysed to identify potential compromises or inappropriate use of your service c. The service provider takes prompt and appropriate action to address incidents Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.	Y	Done by AWS
			The Service User should:-		
			1. Put in place appropriate monitoring solutions to identify attacks against their applications or software.	Y	See section 2.6.8 above
5.4	**Incident management**		The Cloud Provider should:-		
			1. Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001.	Y	Done by AWS. Security incidents only at platform

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
	Ensure you can respond to incidents and recover a secure, available service		Prove that the scope of certification includes incident management controls in detail showing that:- a. Incident management processes are in place for the service and are actively deployed in response to security incidents b. Pre-defined processes are in place for responding to common types of incident and attack c. A defined process and contact route exists for reporting of security incidents by consumers and external entities d. Security incidents of relevance to the Service User will be reported in acceptable timescales and formats Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.		level. 2 factor authentication for all people with access .
			2. Demonstrate robust, well tested and rehearsed incident management procedures.	Y	Done by AWS
			The Service User should:-		
			1. Put in place monitoring solutions to identify attacks against their applications or software.	Y	Knowarth does not access the postgres and MySQL databases except for automated processes, backups can't be stored anywhere except AWS. Access to databases would be logged and reported every 2 weeks.

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
			2. Have an incident management process to rapidly respond to attacks.	Y	Incident management process for Knowarth is in place. Most AWS activities are automated, only certain access permissions are available. LogicalOutcomes test plan in development. For example, DHIS2 access panel is only accessed by LogicalOutcomes team and DHIS2 logs can show us who accessed it on our side.
6	**Personnel security** *Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.*	Personnel screening performed	The Cloud Provider should:-		
			1. Operate a personnel screening process and+ show ISO / CSA compliance to validate the process. Demonstrate that the assessment was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.	Y	Done by AWS
			The Service User should:-		
			1. Ensure IT admin staff are strongly authenticated.	Y	Done by Knowarth
			2. Have a suitable auditing solution is in place to record all IT admin access to data and hosting environments.	y	Done by AWS
7	**Secure development** *Services should be designed and developed to identify and mitigate threats to their security.*	Independent review of engineering approach against recognised secure development standard	The Cloud Provider should:-		
			1. Hold and maintain certification to: a) CESG CPA Build Standard, OR b) ISO/IEC 27034, OR c) ISO/IEC 27001, OR d) CSA CCM v3.0.	Y	Done by AWS

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
	Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.		Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST or CSA STAR scheme.		
8	**Supply chain security** *The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.*	Assessed through application of appropriate standard	The Cloud Provider should:-		
			1. Hold and maintain certification to: a) ISO/IEC 27001, or b) ISO/PAS 28000:2007 Demonstrate that certification was performed by a suitably qualified expert party such as those certified under the CREST scheme.	Y	Done by AWS
			2. Prove that the scope of certification includes supply chain security showing:- a) How your information is shared with, or accessible to, third party suppliers and their supply chains. b) How the service provider's procurement processes place security requirements on third party suppliers. c) How the service provider manages security risks from third party suppliers. d) How the service provider manages the conformance of their suppliers with security requirements.	Y	Done by AWS
			e) How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.		

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
9	**Secure user management** *Your provider should make the tools available for you to securely manage your use of their service.* *Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.*				
9.1	**Authentication of [admin] users to management interfaces and support channels** *In order to maintain a secure service, [admin] users need to be properly authenticated before being allowed to perform management activities, report faults or request changes to the*	Strong authentication in place, which is subject to regular exercising	The Cloud Provider should:-		
			1. Provide Supplier Assertions regarding their approach to strong authentication.	Y	
			2. List all the channels by which the service provider would accept management or support requests from you (telephone phone, web portal, email etc.).	Y	
			3. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'Authentication of users to management interfaces and support channels'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Y	

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
	service.		The Service User should:-		
			1. Ensure that a list of authorised individuals from your organisation who can use those mechanisms is maintained and regularly reviewed.	Y	
			2. Use 2FA to obtain access to the system.	Y	Virtual work spaces for LogicalOutcomes accounts. Knowarth accounts - use their existing security controls.
			3. Configure logging of access attempts.	Y	
			4. Regularly review the access attempts to identify unusual behaviour	Y	
9.2	**Separation and access control within management interfaces** *Many cloud services are managed via web applications or APIs. These interfaces are a key part of the service's security. If [admin] users are not adequately separated within management interfaces, one [admin] user may be able to affect the service, or modify the data of another.*	Access control implemented in software, subject to regular testing	The Cloud Provider should:-		
			1. Provide Supplier Assertions regarding how management interfaces are protected and what functionality they expose.	Y	
			2. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'Access Control to management Interfaces'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Y	
			The Service User should:-		
			1. Ensure that authorised individuals from your organisation who can use those mechanisms are managed by the 'principle of least privilege', typically using a RBAC mechanism.	Y	
10	**[End User] Identity and authentication** *All access to service interfaces should be constrained to*	Two factor authentication OR	The Cloud Provider should:-		
			1. Allow users to authenticate with a username and either a hardware/software token, or 'out of band' challenge (e.g. SMS)	Y	
			2. Provide details of the authentication scheme.	Y	

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
	authenticated and authorised [end user] individuals.	TLS client certificate OR Identity federation with your existing identity provider	3. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the '2FA'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Y	
			The Cloud Provider should:-		
			1. Show that they use TLS 1.2 or above with an X.509v3 client certificate that identifies an individual user.	Y	
			2. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'TLS 1.2+ using an X.509v3 client certificate' Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Y	
			The Service User should:-		
			1. Ensure the secure creation and management of certificates.	Y	
			2. Ensure there are safeguards in place on end user devices to protect them.	Y	
			3. Implement processes to revoke lost or compromised credentials.	Y	
			The Cloud Provider should:-		
			1. Provide support for federating to another authentication scheme, such as a corporate directory, an OAuth or SAML provider.	Y	
			2. Provide details of the authentication scheme.	Y	
			3. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'identity federation'.	Y	

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
			Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.		
			The Service User should:-		
			1. Only use this approach if their existing identity provider uses twofactor authentication.	Y	
11	**External interface protection** *All access to service interfaces should be constrained to authenticated and authorised individuals.*	Internet AND/OR Community network AND/OR Private network	The Cloud Provider should:-		
			1. Implement a Protective Monitoring solution.	Y	
			2. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'external interface protection'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Y	
			The Service User should:-		
			1. Ensure their system has Web Application Firewall (WAFs) protection. This may be provided by the Cloud vendor or a third party.	Partial	See section 2.6.8 above
			2. Ensure that the implemented design protects data by ensuring it is at least two 'firewall' hops from the external network, architected in such a way that the compromise of one firewall will not affect the other.	N	AWS firewall - only one hop from external network but well designed. In opinion of Knowarth DevOps, the AWS firewall is adequate for prevention of compromise
			3. Correctly implement firewall rulesets using the *"Deny All" First* and then *Add Exceptions* principle.	Y	
12	**Secure service administration** *Systems used for administration of a cloud service will have highly privileged access to that service.*	Known service management architecture	The Cloud Provider should:-		
			1. Provide Supplier Assertions regarding their service management architecture.	Y	Done by AWS
			2. Ensure access is only available over a secure channel.	Y	Done by AWS
			3. Limit management actions to authorised staff.	Y	Done by AWS
			4. Audit all management actions.	Y	Done by AWS

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
	Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data. *The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service. If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.*		5. Regularly (daily) review the logs to identify any irregular activities.	Y	Done by AWS
			6. Have separate user accounts for administration and normal user activities. They should not user their administration accounts for normal business activities.	Y	Done by AWS
			7. Not be able to browse the internet or open their external email in the same processing context as they manage systems.	Y	Done by AWS
			8. Protect the integrity of the end user devices used to manage the service.	Y	Done by AWS
			9. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'secure service administration'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Y	Done by AWS
13	**Audit information for users** *You should be provided with the audit records needed to monitor access to*	Data made available	The Cloud Provider should:-		
			1. Record system events in near real-time to provide an audit log.	Y	Done by AWS
			2. Ensure that the audit logs are tamperproof.	Y	Done by AWS
			3. Ensure that the retention period for the logs can be defined by the customer.	Y	Done by AWS

Ref	Security Principle	NHS Recommended Approach	NHS Guidance	LimeSurvey, DHIS2 SIS Production	Comments
	your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.		4. Provide a secure facility to forward / export the logs off the cloud infrastructure.	Y	Done by AWS
			5. Provide facilities to allow logs pertaining to their own systems to be human readable.	Y	Done by AWS
			6. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'auditing facility'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Y	Done by AWS
			The Service User should:-		
			1. Use the audit data as part of an effective pro-active monitoring regime.	Y	Joint responsibility of Knowarth and LogicalOutcomes - testing plan in development
14	**Secure use of the service** *The security of cloud services and the data held within them can be undermined if you use the service poorly.* *Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.*	Enterprise managed devices AND/OR Partner managed devices AND/OR Unknown devices	The Service User should:-		
			1. Use a security hardened master operating system image to build guest servers.	Y	Knowarth
			2. Utilise integrated security monitoring and policy management facilities to help detect threats and weaknesses, due to poor design or mis-configuration.	Y	LogicalOutcomes and Knowarth set access controls to virtual work spaces, review by O365 DLP and Cloudtrail. Testing plan in development.
			3. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'security monitoring'. Ensure that the test is conducted by a suitably qualified provider such as those certified under the CREST scheme.	Y	LogicalOutcomes role