ICT Asset Recovery Standard 8.0

Part 1: Introduction and Explanatory Notes

Released 21.06.2021

Territory Release: United Kingdom

Publication Schedule.
Version 8.0 v3.0 21.06.2021

Standard Owner.
ADISA Certification Limited
UK Company Registration Number 07390092
Data Controller Registration ZA239175

www.adisa.global
www.adisarc.com

1.0 Scope

1.1 Territorial Scope

This Standard applies to the processing of data relating to individuals in the United Kingdom undertaken by data processors established in the United Kingdom.

1.2 Material Scope

This Standard applies to the processing activity of data sanitisation of storage media which is undertaken by a data processor on behalf of a data controller or a sub-processor on behalf of a data processor. The data which resides on that media might be encrypted and will include personal data, criminal conviction data, and special category data as well as corporate data. The Standard assesses risk to the rights and freedoms of the data subject in terms of the right to privacy by ensuring the protection of personal data. Where risk to those rights has been identified, criteria have been developed to assess risk mitigations to protect those rights.

Specific requirements under the UK GDPR are presented as Section 2 within Part 2 of this Standard. Section 3 provides the risk-based evaluation of appropriate technical and organisational measures which the applicant has put in place to protect the physical asset and apply techniques to comply with the data processing requirement of data sanitisation.

1.3 Target of Evaluation of the Standard

This Standard assesses the business process of ICT asset recovery which includes the data processing activity of data sanitisation. The applicant will be a data processor who provides these services to data controllers or who acts as a sub-processor to another data processor. The sanitisation services will be carried out on all categories of data or as determined per customer specification captured within Part 2 Section 2 Criterion 2.1.2 within this Standard.

The service under evaluation will include all systems and processes relating to the ICT asset recovery services, including the processing activity itself and data sanitisation. Processes in scope include customer engagement, logistics services, storage, asset management, and recycling or resale of ICT equipment.

It is imperative to undertake a data mapping exercise to ensure the applicant fully understands what data types, systems and processes are involved in carrying out the ICT asset recovery and data sanitisation services.

During the application process, the applicant will be required to define the processing activities being presented for certification in terms of the types of data being processed (e.g., special category data, criminal offence data, etc.), systems and processes used, including a clear start of that process and a clear ending. This shall include sanitisation services by media type (Part 2 Section 3 Criterion 3.4.1) and data processing carried out on controller or processor premises. (Part 2 Section 3 Module 5). Furthermore, where there are interdependent processing operations such as systems / processes shared with other areas of the business or carried out by third parties, these are to be identified and highlighted during the application process.

1.0 Scope

1.4 Activities out of scope

This Standard only applies to applicants in their capacity as a data processor / sub-processor. The data processing activity is that of data sanitisation which can occur during an end of life, end of rental, or an end of lease asset recovery service or a maintenance service where non-functioning data carrying devices are recovered and the device is NOT destined to be returned to the data controller.

Examples of other services which are not in scope within this Standard would be.

- Resale of new hardware as there is no personal data included in new hardware provisioning,
- Repair services where data sanitisation is not part of the required service.

If the applicant performs other services, it is imperative to disclose these during the application process so that the services being evaluated can be clearly defined.

Activities for which they are defined as a data controller, for example HR data, are also out of scope.

2.0 Normative References

The following documents, in whole or in part, are normatively referenced in this Standard. The criterion against which these documents should be considered are highlighted in the relevant section. The complete list is as follows:

Guidance for completing a Records of Processing Activities.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/#how

Guidance on how to understand categories of data.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data

Guidance on appointment of a data protection officer.
https://ico.org.uk/for-organisations/accountability-framework/leadership-and-oversight/whether-to-appoint-a-dpo/

Guidance on the transfer of data to a third country.
https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/data-protection-at-the-end-of-the-transition-period/the-gdpr/international-data-transfers/

Guidance on paying the data protection fee.
https://ico.org.uk/for-organisations/data-protection-fee/

Guidance on CCTV
https://ico.org.uk/for-organisations/data-protection-self-assessment/cctv-checklist/

Guidance on what goes into a privacy notice.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-privacy-information-should-we-provide/#what2

Guidance on Data Controller and Data Processor Contracts.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

Current NSA approved degausser list.
https://www.nsa.gov/Portals/70/documents/resources/everyone/media-destruction/NSAEPLMagneticDegaussers%20June2019.pdf?ver=2019-07-03-090458-077

ADISA Research Centre Product Claims Test.
https://adisarc.com/product-claims-test/

International Standards
ISO 9001 Quality Management https://www.iso.org/iso-9001-quality-management.html
ISO 14001 Environmental Management https://www.iso.org/iso-14001-environmental-management.html
OHSAS 18001 or ISO 45001 Occupational Health and Safety https://www.iso.org/iso-45001-occupational-health-and-safety.html
ISO 27001 Information Security Management https://www.iso.org/isoiec-27001-information-security.html

3.0 Terms and Definitions

The following are terms referred to within this Standard. Where any terms used are defined within the UK GDPR, the precise same definition is adopted within this Standard and will be sourced as such. The only deviation from UK GDPR definitions as defined by Article 4, is the use of third party and sub-processor definitions which are defined for the purposes of this Standard here.

'applicant' is used to describe any company which wishes to become certified against this Standard.

'asset disposal / asset recovery / asset retirement / asset recycling' are all terms which are used to describe the act of collecting used IT equipment from businesses and then processing them in different ways to deliver a range of services. This can include data sanitisation, product remarketing, and material recycling.

'CESG – Communications-Electronics Security Group' was the UK Government's National Technical Authority for Information Assurance (IA). The name CESG is no longer used following the formation of the National Cyber Security Centre (NCSC).

'chain of custody' is the audit trail which shows who has control over the physical asset at every stage. Without the chain of custody being in place asset management cannot be performed effectively and should any issues arise incident reporting is extremely challenging.

'controller / data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. (Source: UK GDPR) (See also Section 5)

'commissioner' means the UK Information Commissioner's Office.

'customer' means the organisation who is directly employing the services of the applicant. This can be the data controller themselves or another data processor.

'data erasure / data destruction / data sanitisation' means the process, which is performed on data carrying media to render the data, which was formally resident on that media to be no longer recoverable. These processes can include crypto erase, data overwriting, degaussing, or a physical destruction process.

'DIAL' means the Data Impact Assurance Level as determined by the data controller following the method outlined in Section 6..

'degaussing' is a sanitisation technique using a specialist device called a Degausser which emits a magnetic field measured in units of Gauss or Oersteds (Oe). It has the objective of removing the magnetic properties of the coating on the platter of magnetic hard drives or tape surface.

'EEE – Electrical and electronic equipment' means equipment that is dependent on electric currents or electromagnetic fields to work properly. To include equipment for the generation, transfer and measurement of such currents and fields and designed for use with a voltage rating not exceeding 1,000 V for alternating current and 1,500 V for direct current.

3.0 Terms and Definitions

'UK GDPR' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [(United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and see section 205(4))].

'hub' means a location used in the logistics process where consignments are held on an interim basis before being shipped on to the final processing facility. Hubs might be operated by a logistics third party, the ITAD or a designated partner.

'incineration' is a sanitisation technique which is undertaken on each approved media type with the objective of destroying the media by burning it to extreme temperatures so the data cannot be recovered or accessed following the activity.

'ITAD – Information Technology Asset Disposal or Information Technology Asset Disposition' is a service, which facilitates the removal of IT assets from organisations and sanitises the media on which data is stored before either product / component re-use or re-cycling takes place. The companies providing these services are colloquially called ITADs and for the purposes of this Standard the term 'applicant' is used to describe a data processor or a sub-processor who wishes to become certified.

'media' is a term used to describe products which have been manufactured to store data. These are often built into other products such as PCs and laptops. Media typically refers to items referred to in Part 2 Section 3 Module 4.

'member' is a term used to refer to a company which has passed their first audit against this Standard.

'NAND' is the most common type of flash memory and is used in devices such as solid-state drives, and USB flash drives. It is non-volatile so retains data when powered off.

'NCSC – National Cyber Security Centre;' the UK's authority on cyber security and is part of GCHQ. The NCSC brings together and replaces CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI). Full details about the NCSC and their services can be found at https://www.ncsc.gov.uk/.

'NIST – National Institute of Standards and Technology' is an agency of the US Department of Commerce with an extremely wide remit. www.nist.gov.

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. (Source: UK GDPR.)

3.0 Terms and Definitions

'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. (Source: UK GDPR.)

'processor / data processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. (Source: UK GDPR.)

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (Source: UK GDPR.)

'recycling' means the recycling of a product, or part of a product, back into constituent material parts to enable further separation and return of material into the manufacturing-processing stream. Excluding energy recovery, which means the use of combustible waste as a means of generating energy through direct incineration with or without other waste but with recovery of the heat.

'reuse' means the operation by which WEEE/E-WASTE and UEEE or constituent components are used for the same purpose for which they were conceived, including the continued use of the equipment or constituent components which are returned to collection points, distributors, recyclers or manufacturers.

'sanitisation' see data erasure**.**

'shredding' is a sanitisation technique which is undertaken on each approved media type with the objective of destroying the media by cutting it using blades or teeth such that data cannot be recovered or accessed following the activity.

'software overwriting' or 'overwriting' is a sanitisation technique which is undertaken on each approved media type with the objective of writing data to each addressable part of the media to ensure that pre-existing data is overwritten and therefore cannot be recovered or accessed following the activity.

'sub-processor' means any company which provides data sanitisation services to the data processor.

'sub-processing' means any data sanitisation service provided to the data processor by another data processor (who will be a sub-processor).

3.0 Terms and Definitions

'third party' means a company who supports the applicant in the supply of the data processing services but does NOT provide any service which impacts on the data. Examples of this could be a logistics supplier.

'transfer of custody' means the stage at which the processing partner becomes the designated custodian of the assets and becomes responsible for its control and security. These stages need to be clearly agreed and details as to how the assets are verified during the transfer are essential.

'transfer of ownership' means the stage at which the processing partner becomes the owner of the assets being processed. Typically, this coincides with confirmation of the value of the asset(s) and is a point in time agreed on a commercial basis.

'WEEE – Waste Electrical and Electronic Equipment' means all any electronic equipment which has been designated as Waste with the company making this determination being classed as the Waste Producer. Electronic equipment includes all components, sub-assemblies, and consumables, which are part of the product at the time of discarding.

4.0 Alignment to the UK GDPR

The ADISA ICT Asset Recovery Standard 8.0 helps data controllers and data processors / sub-processors understand how to manage compliance within the process of asset recovery. The applicant for certification to this Standard will be a data processor or sub-processor who performs data sanitisation services on behalf of a data controller or their data processor.

Below is a high-level analysis of this Standard against each article within the UK General Data Protection Regulation (UK GDPR) and it cross references the articles against the relevant part of the Standard to indicate how this Standard can help achieve regulatory compliance.

The UK GDPR has 67 Articles, and the following provides a high-level overlay of where the Standard relates to each.

Article 1 Subject Matter and Objectives.
This article relates to the UK GDPR itself so is out of scope for this Standard.

Article 2 Material Scope.
Article 3 Territorial Scope.
These articles relate to the UK GDPR itself so are out of scope for this Standard although the material and territorial scope for this Standard is determined within Part 1 Section 1 Scope.

Article 4 Definitions.
For this Standard these are defined within Part 1 Section 3 Terms and Definitions. Where terms are used which are defined within the UK GDPR the same definition has been adopted and used for this Standard. There is an exception concerning third party and sub-processors which are further defined to avoid any confusion.

Article 5 Principles.
The UK GDPR outlines six data protection principles which must be complied with when processing personal data which are covered extensively within the Standard. These principles are laid out in Article 5 (1):

a) **Lawfulness, fairness and transparency – you must process personal data lawfully, fairly and in a transparent manner in relation to the data subject.**
Whilst this Standard targets data processors or sub-processors who do not have direct contact with the data subject, a core focus is that the processing activities are undertaken in a fully transparent manner to the data controller which assists the data controller in ensuring that they fully understand the data processing being undertaken on their behalf.

b) **Purpose limitation – you must only collect personal data for a specific, explicit, and legitimate purpose. You must clearly state what this purpose is, and only collect data for as long as necessary to complete that purpose.**
This principle is applied by ensuring that the data processor / sub-processor have no access to the controller data and cannot process that data for any other purpose other than for data sanitisation.

4.0 Alignment to the UK GDPR

c) **Data minimisation – you must ensure that personal data you process is adequate, relevant, and limited to what is necessary in relation to your processing purpose.**
This principle is not within scope as the data processor / sub-processor does not access the controller data at any time and has no control over the data being collected.

d) **Accuracy – you must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that you erase or rectify erroneous data that relates to them, and you must do so within a month.**
This principle is not within scope as the data processor / sub-processor does not access the controller data at any time and is therefore unable to be responsible for the accuracy of that data.

e) **Storage limitation – You must delete personal data when you no longer need it. The timescales in most cases are not set. They will depend on your business' circumstances and the reasons why you collect this data.**
This principle is included within Part 2 Section 3 Module 3 Criterion 3.3.44, 3.3.45, 3.3.46, and 3.3.47 which determines the length of time for assets to be processed.

f) **Integrity and confidentiality – You must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.**
It is this principle where this Standard's main UK GDPR compliance focus is. As a large percentage of infrastructure which is used during business operations holds data, the process of asset recovery and data sanitisation is critical to the overall compliance with this principle. Without control over the data sanitation process at the retirement of assets, the controller is allowing uncontrolled risk to be applied to the physical infrastructure and therefore the still resident data. The importance of the industry who provide data sanitisation as a data processing service is of extreme importance for controller compliance against this principle.

Article 6 Lawfulness of processing.
Specific reference to any processing carried out by a competent authority is include within Part 2 Section 2 Module 3 Criterion 2.3.2.

Article 7 and 8 Conditions for Consent, including child consent.
This article is not applicable within this Standard as controller is responsible for complying with conditions for consent.

Article 9 Processing of Special Categories of personal data.
This article is not applicable within this Standard as the controller is responsible for complying with conditions surrounding special category data processing. However, specific reference to any processing carried out by a competent authority is include within Part 2 Section 2 Module 3 Criterion 2.3.2.

4.0 Alignment to the UK GDPR

Article 10 Processing of personal data relating to criminal convictions and offences.
This article is not applicable within this Standard as the controller is responsible for complying with conditions surrounding processing of data relating to criminal convictions and offences. However, confirmation that such a basis has been identified by the controller is measured in Part 2 Section 2 Module 3 Criterion 2.3.2.

Article 11 Processing which does not require identification.
This article is not applicable within this Standard.

Article 12 Transparent information, communication, and modalities for the exercise of the rights of the data subject.
This article is not applicable within this Standard as the data processor / sub-processor has no knowledge of the data which is on the storage media being processed and the processing activity is to sanitise the storage media to stop retrieval of data. In this regard, the data processor / sub-processor will not be able to assist a data controller in the response to a DSAR made on them as they do not know the data on the storage media being processed. Within the Standard, provision is made to permit the data controller to recall storage media should they identify that there is data on that media which they wish to access themselves. This window is very small as the Standard requires all processing activities to be completed within 45 working days unless a longer processing window is permitted by the data controller.

Article 13 Information to be provided where personal data is collected from the data subject.
This article is not applicable within this Standard.

Article 14 Information to be provided where personal data has not been collected from the data subject.
This article is not applicable within this Standard.

Article 15 Rights of access by the data subject.
Article 16 Right to rectification.
Article 17 Right to erasure. (Right to be forgotten.)
Article 18 Right to restrict processing.
Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing.
Article 20 Right to data portability.
Article 21 Right to object.
Please see article 12 for an explanation why these articles are not applicable to this Standard.

Article 22 Automated individual decision-making including profiling.
This article is not applicable within this Standard.

Article 23 Restrictions.
This article is not applicable within this Standard.

4.0 Alignment to the UK GDPR

Article 24 Responsibility of the Controller.
This article outlines the responsibility of the controller including commitment to implement "appropriate technical and organisational measures". The entire premise of this Standard is to identify where risk to the physical asset exists and to then require a minimum level of countermeasure to be put in place to reduce that risk. In addition, this Standard looks at the technical risk to the media and ensures that the sanitisation process is fit for purpose with suitable quality check wrap arounds to provide a layered approach to the processing activity. As a result, this Standard when used as part of a supplier specification will provide the controller with confidence that the data processor / sub-processor selected undertakes the services using appropriate technical and organisational processes. In addition, any data processor / sub-processor who holds this certification will be able to provide evidence that they can provide sufficient guarantees on the robustness of their service by means of the certification held.

Article 25 Data Protection by Design and by Default.
Compliance with this Standard enables the data processor / sub-processor to evidence to the controller that the data processing activities have data protection embedded into it thus enabling the controller to evidence data protection by design and by default within this business process.

Article 26 Joint Controllers.
This article is not applicable within this Standard.

Article 27 Representative is of controllers or processors not established in the United Kingdom.
This article is not applicable within this Standard as the data processors / sub-processors are all established within the United Kingdom.

Article 28 Data Processors.
Part 2 Section 3 identifies where risk within the data processing activity might exist and lists risk treatments as specific criteria. Adherence to this section will evidence that the processor has taken appropriate technical and organisational measures (Article 5 (1) f) to mitigate that risk. This will enable the processor to provide sufficient guarantees to the data controller as per Article 28 (1).

Part 2 Section 2 Modules 8, 9 and 10 all assess the use of sub-processors (Article 28 (2)) plus operating as a sub-processor. (Article 28 (4)).

Article 29 Processing under authority.
This reaffirms that the data processor can only process data when instructed to do so by the controller and is covered within Part 2 Section 2 Module 1 Criterion 2.1.3.

Article 30 Records of Processing Activity.
This article requires that the controller and processor shall maintain a record of processing activities. This is covered within Part 2 Section 2 Module 3 Criterion 2.3.1.

Article 31 Cooperation with the Commissioner.
Controllers and processors, and where applicable, their representatives, shall cooperate on request with the Commissioner in the performance of the Commissioner's tasks. This is covered within Part 2 Section 2 Module 4 Criterion 2.4.2 where the applicants commit to co-operating with the UK Information Commissioner's Office in the performance of its tasks.

4.0 Alignment to the UK GDPR

Article 32 Security of processing.
This article looks at the ability of the controller or processor to secure data during processing activities. Part 2 Section 3 covers risk management within the process, and it introduces Data Impact Assurance Levels (DIAL) which are controller determined. This enables the data processor / sub-processor to put in place countermeasures which are commensurate to the controller's own requirements.

Article 33 Notification of a personal data breach to the Commissioner.
Part 2 Section 2 Module 4 looks at incident management and includes a reporting process to be agreed between processor and controller.

Article 34 Communication of a personal data breach to the data subject.
This is covered in Part 2 Section 2 Module 4 Criterion 2.4.1.

Article 35 and 36 Data Protection Impact Assessment.
Data Protection Impact Assessment (DPIA) is a formal process which is mandated to be done where the processing is likely to result in a high risk to the individuals. In addition, it is a recommended good practice for any major project. The responsibility for undertaking a DPIA resides with the data controller, so for the purposes of this Standard this is out of scope, but the entire Standard can be used to help the controller review and assess risk during this processing activity.

Article 37 Designation of the Data Protection Officer. (DPO)
Article 38 Position of the DPO.
Article 39 Tasks of the DPO.
These articles relate to the appointment of a data protection officer and their subsequent roles. Part 2 Section 2 Module 5 covers all aspects of this.

Article 40 and 41 Code of Conduct and monitoring of adherence.
This article is not applicable to this Standard.
Article 42 Certification.
ADISA Standard 8.0 has been approved by the Commissioner under this article.
Article 43 Certification Bodies.
ADISA Certification Limited have been approved by the UK Accreditation Service (UKAS) to operate as a Certification Body against ADISA Standard 8.0.

Article 44 General principles for transfers.
Article 45 Transfers on the basis of an adequacy decision.
Article 46 Transfers subject to Appropriate Safeguards.
Data Transfers outside of the country of origin are assessed under part 2 Section 2 Module 6.

Article 47 Binding Corporate Rules.
Where processors or sub-processor are subject to Binding Corporate Rules those rules must not put the processor or sub-processor into a position of non-conformance with any Essential or DIAL 1 criteria within this Standard.

All other Articles within UK GDPR are not applicable within this Standard as they cannot be applied to the data processing activities covered under this Standard.

5.0 Information Governance

Within every data protection process there is a requirement for the overall governance of the process to be clearly set out with specific roles and responsibility allocated to participants to ensure the process is maintained to achieve consistent and repeatable results.

Within the business process of ICT Asset Recovery there can be many separate entities involved in the process and the performance of each is imperative to ensure the data processing objective of the business process is achieved – data sanitisation.

This section introduces the participants within this business process and illustrates how information governance can be achieved by each identified participant.

5.1 Data Controller

The data controller is the most important participant within this business process as it will make many of the determining decisions which will shape the process and those involved in the process. The role of the data controller is therefore to present a specification for the business process which subsequent participants are required to meet.

The use of Part 2 of this Standard is designed to provide assistance to the data controller when seeking to identify risk within this process and to ensure appropriate risk treatments are taken by the data processor and / or sub-processor.

5.2 Data Processor

The data processor is the company who has the direct relationship with the data controller and who is contracted by the data controller to perform the required data processing activity – data sanitisation. The processor might perform this activity itself or might use a sub-processor but in either case they are ultimately responsible for the operational compliance of the business process. Part 2 provides clear guidance on how they can identify and then treat risk which pervades this process. As the process is very transactional based, continued vigilance is required and therefore an ongoing audit process to evaluate continued compliance against this Standard is required.

The processor must ensure key staff have a good understanding of this Standard and of the policies and procedures in place at the processor to meet this Standard. They must also ensure that all staff have been trained and undergo continued evaluation against those processes.

Any third parties which are appointed must be assessed and undergo continued evaluation to ensure the requirements set out within this Standard are met.

The data processor should also ensure that the data controller is provided with regular updates on changes to this business process which could impact on previously held positions and could require a change in policy to ensure current best practice is being maintained.

5.3 Sub-Processor

A sub-processor is an organisation appointed by the data processor to perform all or part of the data processing activity – data sanitisation. The sub-processor must hold the same contracted terms as agreed between the controller and processor and must perform the data processing activities in accordance with the criteria laid out within this Standard.

6.0 Data Impact Assurance Levels (DIAL)

Risk can never be removed entirely from a business process and asset recovery is no different. As it is a very physical process, the countermeasures which are put in place can vary and typically result in higher costs for lower risks to the data controller. To ensure the data controller can control their own risk without being determined by cost alone, a new concept is introduced within this Standard which is that of Data Impact Assurance Levels. (DIAL)

The DIAL is derived by the data controller's own view on the following.

- Threat.
- Risk appetite.
- Category of data.
- Volume of data.
- Impact on them of a data breach.

Each of these variables must be determined by the data controller which will provide them with an overall DIAL rating. This in turn will determine what level of service must be provided by the ITAD to meet the DIAL rating.

As the DIAL rating must be a controller decision the ITAD must have it verified as per 3.1.1 within Part 2 of this Standard. To allow this ADISA has a web portal which the controllers can use to create their DIAL rating. This portal produces a certificate which a unique reference and scope of the DIAL as a rating can be present for all data controller assets, a specific location or even just one collection. A DIAL rating can only be verified by the use of this portal or by confirmation in writing from the data controller.

Four main variables are assessed to then overlay against the overall impact of a data breach which will then create the DIAL rating for the data controller which can then be used to identify a suitable supplier and specification of service.

6.1 Threat

First variable is threat and will be based on the ADISA Threat Matrix already being used. A data controller must determine who they feel their most likely threat adversary is. This decision can be aligned to the overall Cyber Threat Analysis but must consider the business process itself and whether the data controller feels asset recovery is a specific threat vector which has actors seeking to exploit. Threat will generally be determined by the industry the data controller operates in and the data which it holds which will help identify actors who may seek to gain access to the data for reasons of financial gain, intellectual property theft or any other purpose.

Threat Level	Threat Actor and Compromise Methods
Low	Casual or opportunistic threat actor only able to mount unsophisticated attacks.

6.0 Data Impact Assurance Levels (DIAL)

Threat Level	Threat Actor and Compromise Methods
Medium	Motivated, targeted threat actor such as organised crime or journalists or hackers applying professional methods to access the physical device and / or data.
High	Government-sponsored organisations using sophisticated techniques with unlimited time and resources to access the physical device and / or data.

6.2 Risk Appetite

Second variable is risk appetite which is a metric determined by the level of risk which a company is allows to pervade into business operations in order to achieve its business objectives. ISO 31000 Risk Management refers to risk appetite as the "Amount and type of risk that an organisation is prepared to pursue, retain or take".

A data controller should take a considered review of this business process as there are many functions which can be a source of risk and so the operational countermeasures can be significant and therefore increase cost. Those countermeasures which are outlined in Part 2 Criteria, were created with likelihood as a factor to consider such that exploitation of a likely risk would require more robust countermeasures than a lesser likely risk.

Risk Appetite	Risk Evaluation
Low	All results must lead to no further actions or risk treatments.
Medium	Additional risk treatments are available but at additional cost.
High	Most cost-effective risk management approach which manages risk but has recommendations for additional risk treatments.

6.3 Categories of Data

The third variable concerns the categories of data being processed which are aligned to the categories within the UK GDPR.

Impact	Data Types
Low	Non-confidential data which might be available in the public domain.
Medium	Personal Data and Corporate Data.

6.0 Data Impact Assurance Levels (DIAL)

Impact	Data Types
High	Same as (2) but including special category data, data relating to criminal offences / convictions and / or corporate secret data.

6.4 Volume of Data

The final main variable is the volume of data being processed within the business process. This will enable the data controller to determine the aggregated risk within the business process.

As this business process is focussed on storage media it is the overall storage capacity which is the critical factor here. The data controller will need to determine how much storage is being presented to the ITAD for processing which must be based on overall capacity of that storage rather than a volume count.

Volume	Storage capacity being processed.
Low	A known number of data carrying media are being disposed of which contains a total of under 10Tb of overall capacity of storage.
Medium	A known number of data carrying media are being disposed of which contains over 10Tb of overall capacity of storage.
High	An unknown number of data carrying media are being disposed of.

6.5 Overall Score

The data controller needs to take the identified scores from 6.1 and 6.2 and apply them to this table.

In this worked example a score of 3 is achieved as the threat level and risk appetite are both medium.

Threat	**High**	**3**	**4**	**5**
	Medium	**2**	**3**	**4**
	Low	**1**	**2**	**3**
		High	**Medium**	**Low**
	Risk Appetite			

6.0 Data Impact Assurance Levels (DIAL)

The data controller then needs to take the identified scores from 6.3 and 6.4 and apply them to this table.

In this worked example a score of 3 is achieved as the volume of data is high and the category of data being low from the previous tables

Category of Data	**High**	**3**	**4**	**5**
	Medium	**2**	**3**	**4**
	Low	**1**	**2**	**3**
		Low	**Medium**	**High**
	Volume of Data			

Taking the sum of the two scores the data controller can then identify their overall score which in this example would be 6.

6.6 Business Impact

The data controller should then look at the business impact which a data breach would have on their business. This will be dependent on the type of business, the scale of operations, the profile the business has, and of course, the type of data being processed.

Impact	Business Impact
Low	Press coverage and brand erosion.
Medium	Possible legal action by data subjects and possible regulatory action.
High	Same as (2) but possible share price damage and / or competitive advantage erosion.

6.0 Data Impact Assurance Levels (DIAL)

6.7 Data Impact Assurance Level.

Taking the business impact level determined in 6.6, the data controller can then align it to the overall score determined in 6.5 to identify their overall Data Impact Assurance Level by using this table.

Impact	High	2	2	3
	Medium	1	2	2
	Low	1	1	2
		1-3	4-8	9-10
	Overall Score			

In the worked example if the business impact of a data breach on the company was viewed as medium and with a score of 6, the DIAL rating would be 2. This would mean the data controller could only use a ITAD who has been certified to a DIAL 2 or 3 service capability.

7.0 How to become certified?

Part 2 of the Standard contains the criteria against which each applicant will be assessed and is presented as four sections as follows:

Section 1: Business Credentials.
Section 2: UK GDPR and UK Data Protection Act 2018 Compliance.
Section 3: Risk Management.
Section 4: Non-Data Service.

Within each Section there are modules which focus on a specific area relevant for each section. These are:

Section 1: Business Credentials.
Module 1 Credit Score.
Module 2 Insurances.
Module 3 Policy.
Module 4 Certifications and Permits.
Module 5 Staff.
Module 6 Code of Conduct.

Section 2: UK GDPR and UK Data Protection Act 2018 Compliance.
Module 1 Customer Engagement.
Module 2 Transparency and accuracy of claims.
Module 3 Records of Processing Activities.
Module 4 Incident and Data Breach Management.
Module 5 Information Governance.
Module 6 Data Transfers.
Module 7 Registration.
Module 8 Sub-Processor Disclosure.
Module 9 Using a Sub-Processor. *
Module 10 Operating a Sub-Processor. *

Section 3: Risk Management.
Module 1 Data Impact Assurance Level.
Module 2 Logistics.
Module 3 Processing Facility Capability.
Module 4 Data Sanitisation.
Module 5 Onsite services. *

Section 4: Non-Data Service.
Module 1 Waste Management.
Module 2 Reuse.

**These modules can be scoped out if the applicant does not provide these services or does not use or operate as a sub-processor.*

7.0 How to become certified?

Within each module of the Standard there are a detailed list of the evaluation criteria which get assessed during the certification process. These are broken down into *Essential, Highly Desirable* categories and criterion which are used to assess suitability of the applicant against the Data Impact Assurance Levels.

Essential are those elements of the service which are mandatory to comply with as it is felt they are the minimum service specification that an applicant must meet on order to be viewed as ADISA Certified.

Highly Desirable which are optional but show the applicant is achieving more than the basic requirement and is providing the highest possible quality and levels of service.

Data Impact Assurance Levels 1, 2 and 3. These criteria are used to help evaluate whether the service being offered by the applicant meets the DIAL rating of the users of the service. It is mandated for the applicant to meet all the DIAL 1 requirements to achieve certification and compliance with the DIAL 2 and DIAL 3 requirements will enable them to achieve a higher DIAL rating for their own service and therefore be able to deliver services for those companies with higher DIAL requirements themselves. NB: To achieve a higher DIAL rating for their service, the applicant shall meet all criteria within that DIAL category.

7.1 Audit results and award

To become certified an applicant must pass an ADISA full audit which will have one of the following four results:

Pass with Distinction
Every single *Essential* criterion and all DIAL requirements have been met.
Overall score of 90% or over is achieved.

Pass with Merit
Every single *Essential* criterion and all DIAL 1 and 2 requirements have been met.
Overall score between 75% and 89% achieved.

Pass
Every single *Essential* criterion and all DIAL 1 requirements have been met.
Overall score between 60% and 74% achieved.

Fail
Should the company fail to achieve a Pass, the criterion which are not complied with will be identified within the audit report and the audit non-conformance process followed which is detailed in **ADISA Standard 8.0 Scheme Manual**, see 9.0. The applicant will only be viewed as passing the audit once all essential and DIAL 1 criterion have been met.

7.0 How to become certified?

7.2 Data Impact Assurance Level (DIAL) [1] Licence

After each full audit, an assessment of the capabilities of the applicant against the criteria which have DIAL options will be made. There are 30 separate assessments which have a DIAL 1, 2 or 3 level of service. An applicant must meet all criterion against a specific DIAL reference to be classified as having that DIAL Licence which would mean that any data controller who has identified themselves as, for example, DIAL 3, should only place business with a service provider holding a level 3 award.

7.3 Overall Awards

An applicant under evaluation would only become certified by achieving a result as per 7.1 and they would be issued a DIAL license as per 7.2. This would enable them to disclose their capabilities to data controllers by the issuing of a certified certificate and logo.

[1] See Section 6.0 for further information on Data Impact Assurance Levels.

8.0 Surveillance Audits - Maintaining Certification

Once an applicant has passed their first audit, they become a certified ADISA member. ADISA then evaluates that member on an on-going basis by conducting Surveillance Audits. These audits take place twice a year and are predominately unannounced, (see advance notice below). There are three types of Surveillance Audit.

1. Data Capability Audit. Auditor assesses the certified member's data capability statement and the sanitisation tools which they operate. The auditor selects a range of products / media which have been processed and forensically analyses them on site to assess if data can be recovered. Checks are also made on degausser outputs and screen aperture within shredders if applicable.

2. Process Audit. Here the auditor will assess the process control and will check contamination and segregation throughout. In addition, a sample of at least ten devices will be picked and the paperwork associated with those devices will be requested once auditor leaves site.

3. Security Audit. The auditor will initially try to gain entry to the facility either in a physical sense or by engineering an opportunity to gain access. Once identified the auditor will then assess the sites security features including CCTV and other physical barriers.

Surveillance Entry Refusal

Due to the unannounced nature of the audits, sites under surveillance are permitted one single refusal of entry to allow for business pressures. ADISA will return to the site at any time (including within 24 hours of the first visit) but if a second consecutive visit is refused without good and evidenced reasons, the audit will be classed as a failure and will follow the non-conformance process outlined in **ADISA Standard 8.0 Scheme Manual,** see 9.0.

Advance Notice

For sites which are remote in geographic location, or which have specific security or health and safety measures imposed on them, 48 hours' notice will be given for surveillance audits.

Evidence of compliance

There is an expectation on all certified members that there will be evidence of them performing the tasks outlined in this Standard as evidence of compliance is an imperative to maintain certification. Should no work have been undertaken place for either new or existing certified members for a period of six months a review will take place to decide on whether certification should be withdrawn. This will follow the same appeals process as the non-conformance process outlined in **ADISA Standard 8.0 Scheme Manual,** see 9.0.

8.1 Awards made for Surveillance Audit

Surveillance audits only result in a Pass or Fail based on the areas being assessed and do not impact on the ITAD's overall award given at a full audit. If the result is a FAIL, then the non-conformance process outlined in **ADISA Standard 8.0 Scheme Manual,** see 9.0.

8.0 Surveillance Audits - Maintaining Certification

8.2 Required Full Audit

Should changes to the certified member be identified at audit or disclosed to ADISA by the member, a full audit may be requested by ADISA outside of the three-year regular internal. These full audits will be conducted as per the **ADISA Standard 8.0 Scheme Manual** and will result is an award being issued based on the findings of that audit.

9.0 Audit and non-conformance processes.

Section 7 and 8 of this document provide a high-level introduction to the audit process and expectation on those seeking to achieve or maintain certification. Further details including the non-conformance process can be found in the **ADISA Standard 8.0 Scheme Manual** which is a separate document available from ADISA. Requests for copies can be made by emailing enquiry@adisa.global.

10.0 General Notes

Certified Logos

Each certified company is issued a logo with a unique reference which they can use for their own marketing purposes. A certified company's status can be confirmed via the ADISA website which will always contain the current list of certified companies.

Excluding ADISA's own publications, if the ADISA logo is used for promotional purposes it should be considered as unofficial and unsupported.

Certificates

Each certified company is issued a certificate which includes the unique certified reference number and a validity period. Use of the certificate and logo is only permitted by adherence to this Standard which is confirmed during the audits process.

Disclaimer

- Compliance with the ADISA Standard does not indemnify any party from legal obligations or against legal actions.
- ADISA Certification offers neither guarantee nor indemnity to any organisation utilising the services of the certified member.
- This Certification process is detailed within the **ADISA Standard 8.0 Scheme Manual** and is based on current best commercial practices and might be subject to change. Any change will be made public via ADISA social media channels and website.

Copyright

All information included in this Standard is the property of ADISA except where otherwise referenced. Further reproduction is prohibited unless otherwise authorised in writing.

Further Development

ADISA reserves the right to make major or minor changes to this Standard, but any such changes will follow the process outlined within the **ADISA Standard 8.0 Scheme Manual.**

Phone: + 44 (1) 1582 361743

www.adisa.global
info@adisa.global