ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Released January 1st, 2020

2019 Computing Security Awards WINNER The Compliance Award

Defence INFOSEC DIPCOG CESG Product Co-Operation Group

Foreword

This document (ADISA ICT Asset Recovery Standard 7.0) is presented for use from January 1st, 2020. It is the current version of this Standard which was originally launched in 2010. The owner of this Standard is the Asset Disposal and Information Security Alliance which is an organisation designed to improve risk management and data protection within the business process IT asset retirement.

This Standard followed a review and development process over nine months with the primary objective of aligning it to Data Protection legislation including but not limited to the EU General Data Protection Regulation, the UK Data Protection Act and the Californian Consumer Privacy Act 2018.

The review and development process were undertaken as follows.

- ADISA undertook a review of the 6.0 Standard and drafted a v7.0 Standard between April and June 2019.
- A steering group was formed in July 2019 which included ADISA members and industry professionals. The committee included companies with an international footprint, software overwriting vendors, data protection professionals and information security experts.
- The draft 7.0 rev. 0.1 standard was submitted on 27.07.2019 to the steering group for their consideration.
- An initial review meeting took place on 07.08.2019 and based on discussions with committee members a revised 7.0 rev. 0.2 was issued to the steering group on 28.08.2019 for their consideration.
- A second meeting took place on 26.09.2019 where 7.0 the rev. 0.2 was reviewed from start to finish.
- The draft 7.0 rev. 0.3 was released to ADISA members for consultation on 11.10.2019.
- Draft 7.0 rev. 0.4 was created to clarify wording based on feedback and was re-submitted to ADISA members.
- Draft 7.0 rev. 0.5 was released 30.10.2019 for public consultation.
- ADISA Asset Recovery Standard 7.0 was presented to an ADISA members meeting in London on 28.11.2019 and was proposed, seconded and accepted unanimously for public issue as the current ADISA Standard.
- Released on 31.12.2019 for immediate usage.

Endorsement Notice

The text of ADISA ICT Asset Recovery Standard 7.0 v. 1.0 has been approved by the ADISA Standard Steering Group and the ADISA Membership on November 28th, 2019.

Normative References

There is an in-depth set of guidance notes available to organisations wishing to become certified. These guidance notes explain the purpose of each criterion and provide some context into what would be looked for against each at audit. These guidance notes are not publicly available and request for copies can only be made to ADISA directly via members@adisa.global

Standard Owner

Asset Disposal and Information Security Alliance Limited
31, Thrales End Business Centre, Thrales End Lane, Harpenden, AL5 3NS
UK Company Registration Number 07390092

Introduction

Launched in 2010, ADISA has the objective of improving risk management and data protection within the business process of IT Asset Retirement. This process is commonly referred to as ITAD and an industry has evolved out of the recycling sector to augment material recovery with services such as asset management and data sanitisation. The ADISA ICT Asset Recovery Standard was developed to identify risk which might exist within this process and to then assess countermeasures which are in place to mitigate that risk.

This Standard, and certification to it, should be used as a benchmark for any organisation releasing assets to a partner to process on their behalf when data protection and compliance are paramount.

The Standard is presented in 10 Modules each covering different aspects in asset recovery. Within each module there might be subsections and within each subsection there are mandatory requirements which are Essential Criteria and advisory elements which are Highly Desirable.

The objective of the ADISA Asset Recovery Standard is:

- To ensure that every data bearing asset is managed throughout the process and that any resident data is sanitised in accordance with the client's requirements or to industry best practice levels.
- To promote the re-use of assets through risk management.
- To help organisations comply with Data Protection Laws.

This is achieved by:

- Creating a physical environment within the ITAD process which offers equivalent levels of security to those in place when the asset is in its live environment.
- Testing the abilities of the service provider to create and then maintain the chain of custody throughout the process.
- Ensuring the process is consistent and repeatable.
- Assessing current data sanitisation processes on ALL media types.
- Giving the end user the assurance that ADISA-certified companies are both professional and ethical.

We continue to invite comments and feedback from stakeholders and encourage these to be made to submissions@adisa.global

Best Wishes

Steve Mellings

Founder, Asset Disposal and Information Security Alliance

December 23rd 2019

Contents

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Complying with the Standard

Complying with the Standard

This Standard includes ten separate modules for assessment which are:

- Module 1: Business Credentials.
- Module 2: Client Engagement.
- Module 3: Sub-Processors and Third Parties.
- Module 4: Logistics.
- Module 5: Processing Facility.
- Module 6: Data Sanitisation Capability.
- Module 7: Waste Management.
- Module 8: Product Re-Use.
- Module 9: On-Site Services.
- Module 10: Leasing Companies.

With the exception of Module 10, which is only a requirement for leasing companies, each Module is now mandatory to be assessed as part of certification. Certification CANNOT be achieved by scoping an application for only part of your service. All asset recovery services undertaken by the named applicant will be assessed as part of the certification process.

Certification Criteria

Within each module of the Standard there is a detailed list of the evaluation criteria, which the audit process examines during the certification process. These are broken down into *Essential* and *Highly Desirable* categories.

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

Highly Desirable criteria are those elements, which show the service provider is achieving more than the basic requirement and is providing the highest possible quality and levels of service.

Award made for Full Audits.

There are seven possible outcomes at an ADISA audit, which are as follows:

Pass with Distinction with honours.
Every single ***Essential*** criterion has been met.
Overall score of 95% achieved.

Pass with Distinction
Every single ***Essential*** criterion has been met.
Overall score between 85% and 94% achieved.

Pass with Merit
Every single ***Essential*** criterion has been met.
Overall score between 70% and 84% achieved.

Pass
Every single ***Essential*** criterion has been met.

Conditional Pass
Any company undergoing an audit which falls short of either a pass or of the threshold to the higher level of pass by a narrow margin will be issued with a conditional award and given the chance to address identified shortcomings. Once these remedial works have been completed satisfactorily the final level of pass will be awarded.

Examples of a Conditional Pass:

- The absence of a written document for a particular simple procedure.
- Inaccurate, incomplete or missing information on company reports.
- The utilization of incorrect or inappropriate downstream supplier information on record.

Fail
Should the company fail to achieve a Pass grading the changes required will be made clear within the audit report and ADISA will work with the ITAD to help implement these changes. A free re-audit will be carried out within three months of receipt of the original audit report.

Examples of Fail:
- Inability to meet all the ***Essential*** criteria.
- The absence of the required type of door entry system and investment is necessary.
- Where the company's process does not capture the right type of information early enough and changes to process are required.
- Where the company has not had all their staff correctly vetted.

Rejection
Should the audit identify what the auditor believes to be wholly unacceptable and unavoidable risk the company will be graded with an absolute fail. This will result in the return of 50% of the Certification Fee and the audit report will identify remedial action required before the company will be able to reapply for ADISA Certification.

Examples of Absolute Fail:
- Where part of the company's physical fabric, which cannot be easily changed, fails the audit (e.g. lack of security within their processing area).
- Where the company is found to make false claims regarding their capabilities and/or certifications, which are discovered during the audit.

<u>Awards made for Unannounced Audit</u>

Unannounced audits can result in the following types of award:

- **Pass.**
  All tests passed with no issues.
- **Pass after corrective actions.**
  All tests passed after agreed corrective actions completed.
- **Pass with exceptions.**
  Not all tests resulted in a pass, but there were mitigating reasons why that would be the case. This will be listed on the audit document.
- **Fail.**
  Member failed the audit and the result would follow the audit failure process.

General Notes

Logos

Excluding ADISA's own publications, if the ADISA logo is used for promotional purposes it should be considered as unofficial and unsupported. Each certified member is issued a unique certified logo, which they can use for their own marketing purposes. It is acknowledged that use of logos is difficult to police, so ADISA certified logos are different from company logos. Each one is also numbered to ensure uniqueness.

Disclaimer

- Compliance with the ADISA standard does not indemnify the service provider from legal obligations or against legal actions.
- ADISA certification offers neither guarantee nor indemnity to any organisation utilizing the services of the certified ITAD.
- This Certification process 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

Further Development

ADISA reserves the right to make minor changes to this standard should any significant problem be identified and requires addressing. Any changes will be made public and should these changes impact on existing certified member status then ADISA will re-visit each certified member and review their status against this change. NB: it is neither desirable nor expected for any changes to be made.

ADISA believes that this industry Standard will continue to be developed due to both experience and collaboration with other standards bodies. Comment and critique is welcome and can be made to submissions@adisa.global at any time.

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Module 1

Business Credentials

Module 1 Business Credentials

1.0 Introduction

ADISA has identified several areas within the general governance of a business which might have an implication on the suitability for achieving ADISA certification. This module assesses such areas which are felt to form the foundations of a strong organisational structure from which service delivery can be achieved.

ADISA Module 1 Core Principles.

- Business governance;
    - Financial stability.
    - Insurances held.
    - Confirmation of licences, certifications and permits held.
    - Health and safety.
- Staff screening.
- Incident management.
- Business continuity.

1.0.1 Scope

This module is a pre-requisite for all companies who wish to undergo certification against the ADISA standard and provides a positive indication of the integrity and viability of the business. Any business unable to pass the essential elements within Module 1 should not consider taking part in the ADISA process.

Module 1 Business Credentials

Essential

Ref	Criteria
1.0 a	Companies must be able to show credit worthiness via the successful completion of a credit check, typically a Dun and Bradstreet risk indicator of a minimum of 3. (See Appendix 2.)
1.0 b	Companies must register, if required by law to do so, with any authority within their region which governs data protection. (For example, within UK Data Controller must pay the Data Protection Fee to the Information Commissioner's Office.)
1.0 c	All certifications (such as ISO) must be disclosed and reports verified by ADISA.
1.0 d	All environmental licences and permits required to operate in each region of operation must be disclosed and verified by ADISA for inclusion within the website entry on ADISA site.
1.0 e	Companies must have a Health and Safety Policy and risk assessments of business activities including on-site and off-site work.
1.0 f	Companies must hold Employers Liability Insurance or equivalent in your region.
1.0 g	Companies must hold Public Liability Insurance or equivalent in your region.
1.0 h	Companies must hold Professional Indemnity Insurance, or an equivalent insurance policy, which protects the business from claims arising due to a failure within the service offered. A copy of this policy will be required to be reviewed by ADISA to ascertain whether it is fit for purpose.
1.0 i	Personnel screening policy document must be issued and must include a requirement for all staff who have access to the data processing activities to undergo commercial personnel screening to include the following checks: • Criminal background check. • Proof of ID. • Proof of address. • Proof of ability to work.
1.0 j	All driver's contracts of employment must state that the driver needs to disclose any changes in their licence/permit whilst in the employment of the ITAD.
1.0 k	All employee's contracts of employment must state that the employee needs to disclose any changes in their status (such as criminal convictions or work permit amendments) whilst in the employment of the ITAD.
1.0 l	Companies must hold ISO 9001 Quality Management Systems. The last audit report must be disclosed to ADISA with any non-conformities.
1.0 m	Companies must have a written Business Continuity Policy (BCP) and provide evidence of their most recent test. This BCP needs to include provision for systems failure and facility compromise, for example by flooding, and detail how service provision is maintained.

1.0 n	Organisations must have a documented security incident response procedure. This must include: - Definition of an incident including severity. - Incident Response including disclosure plan. - Incident investigation including root cause analysis.
1.0 o	Each member must sign and comply with the current Member's Code of Conduct.

Highly Desirable

Ref	Criteria
1.0 p	Companies should be able to show credit worthiness via the successful completion of a credit check, typically a Dun and Bradstreet risk indicator of 1 to 2.
1.0 q	Personnel screening should be done every 3 years.
1.0 r	Companies should hold Product Liability Insurance or equivalent in your region
1.0 s	Companies should hold ISO 14001 Environmental Management Standard.
1.0 t	Companies should hold OHSAS 18001 or ISO 45001 Occupational Health and Safety Standard.
1.0 u	Companies should hold ISO 27001 Information Security Management System which includes the ITAD process within scope.
1.0 v	Any ISO's held should be awarded by a recognised auditing body holding accreditation within the regions operated in. For example, UKAS.

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Module 2

Client Engagement

Module 2 Client Engagement

2.0 Introduction

All data processing needs to be undertaken in a fully transparent way not only to ensure that all parties understand the scope of the processing activities but also as a part of all party's own regulatory compliance position. This module looks at how the ITAD engages with their clients and how the services undertaken are agreed to by the client. It also explores the formation of the contract between both parties.

ADISA Module 2 Core Principles.

- Regulatory compliance.
- Transparency between all parties.
- Clear and evidenced agreement for services.

2.0.1 Scope

This module assesses how the ITAD and its clients form their working relationship. Within many data protection laws there are specific requirements for how this working relationship is to be formed and how the services undertaken are controlled. This module has a minimum legal requirement listed as essential but the preferred and recommended position is listed within the highly desirable and this is encouraged.

Module 2 Client Engagement

2.1 Client Paperwork / Process

Essential

Ref	Criteria
2.1 a	Samples of all paperwork used during the customer engagement process must be provided to ADISA and client engagement process agreed. This submission must include but not be limited to: - Documents used to form the contract / written authorisation with the client. - Documents used to manage the collection process. This criterion will be used to generate a workflow which includes details for dealing with variations and this must be signed by both parties to become certified.
2.1 b	Any documents referred to in 2.1 (a) which are created after initial audit or which are changed significantly, must be shared with ADISA within 30 working days of implementation.
2.1 c	In the absence of a signed contract, a written authorisation must be in place between the ITAD and their customer. This authorisation must include details of the service being provided and must include as a minimum; • Confirmation of agreed auditing detail. • Confirmation of approved sanitisation process by media type. • Confirmation of agreement for logistical services to include hub usage and permission for multi-point collections if used during service provision. • Confirmation that the service issuer is the owner of the equipment and that they are legally entitled to release the equipment. • Confirmation of the point within the process where the ITAD accepts custody of the assets and therefore liability. • Designation of the service provider as a Data Processor. • Agreement for the use of any third parties / sub-processors.
2.1 d	Where no contract or written authorisation is in place ITAD must adhere to local legal requirements regarding operating as a Data Processor. For example. In the EU an ITAD cannot operate as a Data Processor without a contract in place and as such any EU ITAD cannot issue certificates of destruction without either 2.1 (c) or (e) being in place.

Highly Desirable

Ref	Criteria
2.1 e	A signed contract or data processing agreement should be in place between the ITAD and their customer. This contract must include details of the service being provided and must include as a minimum: • Confirmation of agreed auditing detail. • Confirmation of approved sanitisation process by media type. • Confirmation of agreement for logistical services to include hub usage and permission for multi-point collections if used during service provision. • Confirmation that the service issuer is the owner of the equipment and that they are legally entitled to release the equipment. • Confirmation of the point within the process where the ITAD accepts custody of the assets and therefore liability. • Designation of the service provider as a Data Processor. • Agreement for the use of any third parties / sub-processors.

2.2 Transparency and accuracy of claims

Essential

Ref	Criteria
2.2 a	Website claims are reviewed and must contain only accurate and true statements.

.

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Module 3

Sub-Processors and Third Parties

Module 3 Sub-Processors and Third Parties

3.0 Introduction

In any business service supply chain, it is generally accepted that the contracted organisation will use partners to provide either primary or secondary parts of the service. Within the IT asset recovery service this could be for the provision of data sanitisation services or in the supply of services to facilitate the ITAD to perform their own service.

Whenever a partner is used to perform part of the data sanitisation service, for example on-site shredding, they are viewed as a sub-processor and must be treated with the same level of scrutiny as the primary data processor.

Whenever a partner is used to facilitate the ITAD's own service, for example logistics, then they are viewed as a third party and must be assessed in a way which is reflective of the impact their service can have on the performance of the ITAD itself.

This module identifies such partner organisations and assesses each against the requirements of the ADISA Standard relevant to the service.

ADISA Module 3 Core Principles.

- Regulatory compliance.
- Control over partner.
- Transparency to client.

3.0.1 Scope

This module looks at the use of third parties and sub-processors within the ITAD process. It's essential for the ITAD customer to understand where sub-processors and third parties are used and for the ITAD to control them.

Module 3 Sub-Processors and Third Parties

3.1 Sub-Processor and Third Parties Disclosure

Examples of sub-processors might be on-site shredding, down streaming of product sets for processing (for example mobile phones) or sending drives for repair. These are all PERMITTED as long as the criterion in 3.1 and 3.4 are met.

Examples of third parties might be logistics service providers or waste management suppliers.

Essential

Ref	Criteria
3.1 a	Each certified member must complete the sub-processor / third party disclosure form and revalidate and submit every 6 months.
3.1 b	Each sub-processor must be approved by ADISA prior to use. This could be by formal certification, by blanket approval or individual case by case approval.
3.1 c	Each third party must be assessed by ITAD to confirm adherence to ADISA Standard prior to use. This could be by formal certifications held or by audit.
3.1 d	The use of a sub-processor / third parties must be disclosed to the client prior to work being carried out. It is not essential to name the sub-processor / third party but to denote their credentials and achieve a blanket approval from customers.

3.2 Third Party Logistics

Essential

Ref	Criteria
3.2 a	Any third parties used to perform any part of the logistics service must be controlled by means of a formal written contract, which includes confirmation that third-party vehicles and service meet all requirements of Module 4.
3.2 b	Any third parties used to perform any part of the logistics service must be audited by the ITAD to ensure compliance with Module 4. This can be done by a third-party or by the ITAD but must result in a written record and contain evidence. Self-validation by the logistics provider is not permitted.
3.2 c	Any third party used to perform any part of the logistics service must meet Module 4 requirements in addition to the following requirements: • Screen staff as per 1.0 (i). • Have a documented security incident procedure as per 1.0 (n).

Highly Desirable

Ref	Criteria
3.2 d	Any third parties used to perform any part of the logistics service should be audited by ADISA to ensure compliance with Module 4.

Module 3 Sub-Processors and Third Parties

3.3 Third Party Waste

Essential

Ref	Criteria
3.3 a	Where the company passes waste to a third-party vendor for treatment, they must be able to show documented evidence that their downstream partner holds all relevant permits and /or licences to collect and treat waste within each region operated in. This record must include validity dates of permits / licences held and copies of current permits / licences held must be kept on file by the ITAD.

3.4 Using a Sub-Processor

A Sub-Processor is a company who undertakes data processing activities on behalf of the ITAD. Examples could be onsite data shredding or hard drive repair.

Essential

Ref	Criteria
3.4 a	Sub-processors must be controlled by a contract which has the same explicit terms which the ITAD has agreed with the client. This is to include all aspects in 2.1 (c).
3.4 b	Any sub-processor used to perform any part of the data processing service must be audited by the ITAD to ensure conformance with ADISA Standard. This can be done by a third-party or by the ITAD but must involve a physical audit and result in a written record. Self-validation by the sub-processor is not permitted.

Highly Desirable

Ref	Criteria
3.4 c	Any sub-processor used to perform any part of the data processing service should be ADISA certified.

Module 3 Sub-Processors and Third Parties

3.5 Operating as a Sub-Processor

This section covers a situation whereby the ITAD operates as a sub-processor on behalf of a Data Processor. Examples could be where the ITAD's services are resold by a channel partner or they collect failed drives for repair from another ITAD.

Essential

Ref	Criteria
3.5 a	Where ITAD operates as a sub-processor they must have the ADISA sub-processor form completed.

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Module 4

Logistics

Module 4 Logistics

4.0 Introduction

Module 4 focuses on the logistics activity associated with the transportation of assets from the client's site to processing facilities. Risk of loss of assets during this process is assessed both in terms of the probability of physical loss or theft but also in terms of control and management of the chain of custody. It is imperative that at the point of collection equipment is controlled, so that verification on receipt is confirmed and the risk of potential losses during logistical transfer is minimised.

ADISA Module 4 Core Principles.

- Control of the asset during the transportation process.
- Physical security of the asset.
- Mitigation of risk throughout the transaction.
- Environmental capabilities.

4.0.1 Scope

This module is designed to assess the capabilities of an ITAD or a third-party courier when collecting IT and Telecommunications assets and transporting them in a secure manner to a processing site.

Module 4 Logistics

4.1 Site Access

A key risk during transportation is the exposure of assets during the movement from the location where they are stored to the vehicle used during transportation. This section assesses how factors which can increase that risk are identified during the engagement process.

Essential

Ref	Criteria
4.1 a	Site access details for each pickup location must be captured in writing and communicated to relevant logistics staff / partners and must include: • Details regarding site access such as parking issues and any height restrictions. • Confirmation of site security requirements such as vehicle driver identification requirements. • Location of items to be collected and details of any stairs etc to inhibit collection. • Details of any oversized or heavy items including UPS and racks to be collected.

Highly Desirable

Ref	Criteria
4.1 b	ITAD should have the ability to perform a formal site survey including templates and methodology. Formal Site Survey should include: • Parking location identified, and any obstructions noted. • Building access route identified and any issues noted. (For example: door height or width). • Detailed inventory list to confirm type and volume of items for pick up. • Dimensions of any oversized item and weight estimate for heavy items including UPS and racks.

Module 4 Logistics

4.2 Hub and Storage Locations

It is often a commercial or geographic reality that the need for hubbing or staging of consignments is required. This is where the assets are stored at a different location whilst on route to the processing facility. These locations are identified as high risk and this section assesses how this risk is disclosed to the client and how it is managed operationally.

NB: If the ITAD does not use hubs then this section is scored as 'not applicable' and the audit summary will state no approved hubs.

Essential

Ref	Criteria
4.2 a	Hub locations must be identified and disclosed during the audit process. Where this is not possible, the ITAD's customer engagement process must include the customer's approval via clear written consent to the use of unidentified hubs during the logistics process.
4.2 b	Hubs must be operated by one company. Where multiple companies operate within the hub, each operator must have a segregated operation from the other. Examples of segregation could be a cage, wall or any other physical barrier which precludes easy access to stored equipment.
4.2 c	Hubs must be operated with a security culture and be able to evidence that suitable policies and certifications are in place. All of these are to be disclosed during the audit process. Where this is not possible, the ITAD's customer engagement process must include the customer's approval via clear written consent to the use of unidentified hubs during the logistics process.
4.2 d	Physical hub security must include, but not be limited to: • Secure outer perimeter. • CCTV on all access points. • Alarm on all pedestrian and vehicle points. • PIR sensors in place to detect motion should physical perimeter be compromised.
4.2 e	Storage security must include, but not be limited to: • Assets to be unloaded and stored under CCTV coverage. • Access control must be in place to ensure areas where assets are stored can only be accessed by authorised personnel.
4.2 f	Chain of custody must be achieved by: • Consignment being booked in using a consignment box count which is to be verified during receipt. • Consignment is to be booked out using a consignment box count which is to be verified during exit.
4.2 g	Where third party hubs are used, consignments must be physically secured against access and must not undergo re-packaging or re-palletisation.

Module 4 Logistics

4.3 Physical Security of vehicles and collection process

Essential

Ref	Criteria
4.3 a	A fleet list must be provided of vehicles operated directly by the ITAD and are used for asset recovery services. Any changes to this fleet require the ITAD to notify ADISA within 30 working days of implementation.
4.3 b	Each vehicle must be GPS tracked which must allow for: • Historical data to be stored for a minimum of six months. • Route history to be available upon request.
4.3 c	Each vehicle must have suitable physical protection such as electronic or mechanical immobiliser and /or an alarm.
4.3 d	Each vehicle must be solid sided and have solid bulkheads.
4.3 e	Customers must have the option to have collections made using vehicles with generic livery (i.e. non-task specific).
4.3 f	Multi-point collections from different customers must include: • Physical separation of loads which is sufficient to maintain segregation and to ensure no load slippage can mix consignments. • Each part of the load to have a unique identifier able to identify the customer.
4.3 g	Where any third-party vehicles are used by the ITAD, for example short-term rentals, there must be written evidence of their conformity with the criteria within this module. This must include details for how the vehicle will be GPS tracked.

Highly Desirable

Ref	Criteria
4.3 h	Each vehicle should be GPS tracked and have the ability to provide: • Stationary alert. • Route control capability (Watch box or geo-fence).
4.3 i	All vehicles should have additional locking security such as slam locks or isolated tail-lifts.
4.3 j	All consignments should be labelled with a unique identifier which cannot clearly identify the customer by name.
4.3 k	Multi-point collections from different customers should include additional security countermeasures such as: • Two operatives. • Lockable totes or crates. • Security tags on each consignment.

4.4 Mitigation of risk during transportation

Essential

Ref	Criteria
4.4 a	All vehicles must be able to communicate with base via telephone or radio.
4.4 b	Each driver must have their driving licence or permit checked annually and details kept on their record.
4.4 c	There must be a written collection process which includes a risk assessment that identifies and mitigates all clear risks. For example; Doors to be closed and locked whenever the vehicle is to be left unattended. This must be included in the driver induction or handbook.
4.4 d	A full method statement must be provided to include, but not be limited to: • Policy for comfort stops. • Policy for refuelling stops. • Policy for breakdown. • Plan for dealing with over and out of hours' situations.
4.4 e	All records of collections made (which include relevant signatures) must be permanently retained by the ITAD (Digital or paper) for seven years.

Highly Desirable

Ref	Criteria
4.4 f	ITAD should operate its own fleet operated by its own staff. Occasional use of third parties for specific requirements or emergencies is permitted.
4.4 g	Each driver should have their driver licence or permit checked every 6 months.

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Module 5

Processing Facility Capability

Module 5 Processing Facility

5.0 Introduction

Companies that offer IT Asset Disposal services come from many different backgrounds and the way in which equivalent services are delivered can vary dramatically, not only company to company but also site to site. For this reason, the assessment of each individual processing facility is essential to deliver an independent verdict on the capability of an ITAD to meet all required elements. This module assesses all aspects of the ITAD processing facility.

ADISA Module 5 Core Principles:

- Managing workflow.
- Protecting the asset.
- Asset management via the establishment of the chain of custody.
- Deploying the tools for sanitisation, which are commensurate to the level of risk.

5.0.1 Scope

This module is designed to assess the capabilities of an ITAD when receiving items for processing at their own facility. This module is only concerned with assessing that capability from the point of receipt. Please review other modules for elements outside of this scope.

Module 5 Processing Facility

5.1 Chain of Custody

Essential

Ref	Criteria
5.1 a	Consignment integrity (Transfer of custody) must be achieved: • The driver must have photo ID available for every collection. • The collection paperwork must include the named individual authorised to release the assets on behalf of client. • A signature, printed name and date, must be obtained from the releasing person or agent on behalf of client. • A signature, printed name and date, must be obtained from the logistics representative. • A signature, printed name and date, must be obtained from the receiving employee of the certified member. • Where hubs are used, consignment must be signed into hub and then signed out of hub.
5.1 b	Chain of custody must be achieved by identifying a count of assets on site which could include identification by a numeric count of products or by number of boxes / pallets in the consignments. This count must be verified and signed for by the client and recipient before leaving the site.
5.1 c	In the absence of a written client specification upon receipt at the facility, loose or separate data carrying media, including tape, must be individually tracked on the system and classified as a separate asset.

Highly Desirable

Ref	Criteria
5.1 d	In the absence of a written client specification, any additional assets including any loose or separate data carrying media found during the process should be quarantined and disclosed back to the client to await direction.
5.1 e	The ITAD should be able to display a comprehensive capability to start the chain of custody at point of collection via the tracking of the asset using a unique reference identifier such as a serial number. This capability should include verification on receipt at the facility and at the end of the process itself.

Module 5 Processing Facility

5.2 Physical Security

ADISA Certification requires that all aspects of the ITAD site must be secured to deter either opportunist intruders or determined planned attacks. As such both physical and technological deterrents need to provide overall site security.

Essential

Ref	Criteria
5.2 a	Facility must have CCTV coverage which permits the identification of individuals via facial details and / or vehicle registration details on the following areas: • All pedestrian access points including fire exits. • Where the vehicles are unloaded to ensure vehicle registration is visible, and visibility of the loads is achieved. • Extensive coverage within the data processing area. • Footage is to have time and date stamp and be synchronised regularly. • Location of external cameras is to be such that tampering by intruders or staff without equipment would be impossible.
5.2 b	Where CCTV is in operation there must be visible and legible warnings that CCTV is in use in locations where it can collect images of employees or members of the public.
5.2 c	CCTV coverage must be recoverable for at least one week. Recorder should be protected from threat of theft, fire and technology failure.
5.2 d	Organisations must have an intruder alarm installed to recognised national standards.
5.2 e	Facility must have alarm points on all pedestrian and vehicle access points. In situations where the latter is not possible then PIR coverage is required.
5.2 f	There must be an alarm response plan which details how the alarm is monitored, what happens when it is triggered and evidence of a clear escalation process.
5.2 g	Alarm response plan must be tested at least once per year.
5.2 h	Personal infrared sensors must be in place to ensure that intrusion would be detected in all main areas of the data processing areas.
5.2 i	Perimeter walks must be carried out weekly and documented to confirm checks are made on: • Buildings in the vicinity to check for change of use or vacant lots. • Position and line of site of all external cameras. • Perimeter fencing (if in place) to check for signs of damage.
5.2 j	Once unloaded, all equipment must be taken inside the premises immediately.

Highly Desirable

Ref	Criteria
5.2 k	CCTV should cover the following areas: • All external aspects to be covered. • Access roads to be covered.
5.2 l	Vehicles should be unloaded such that public cannot view unloading activity which can be achieved by unloading inside the facility or at the threshold of the facility.
5.2 m	Organisations should have motion or thermal detection sensors in place (such as PIR) with extended coverage such as on external walls, all windows and roof.
5.2 n	Facility should have smoke / fog or acoustic intruder system in the processing area.
5.2 o	Organisations should show no external signs of IT activities.
5.2 p	Facility should have designated security guards operating during the day.
5.2 q	The site should have out of hours' physical security coverage which can include alarm and camera monitoring or on-site security guards.
5.2 r	Any obvious points of entry such as easily accessible windows, roof lights etc should have additional security countermeasures such as bars or alarms.
5.2 s	Facility should have exterior fitted Passive Infra-red (PIR) lighting, operating out of hours. (Proximity lighting.)

Module 5 Processing Facility

5.3 Internal Security

One of the main security control challenges is mitigating the potential for insider theft. ADISA will audit internal security countermeasures, staff checks and controls that minimise the risk for potential insider theft.

Essential

Ref	Criteria
5.3 a	The premises must not be shared with any other organisation without significant physical segregation and access controls to be in place.
5.3 b	The premises must not have any other business process operating out of the facility without significant physical segregation and same site security standards to be in place and verifiable.
5.3 c	The data processing facility must have controlled access for authorised staff only.
5.3 d	Non full-time staff (e.g. temporary or contract workers) must not be used in data processing areas unless they have already undergone the same extensive screening as full-time staff or are chaperoned within the data processing areas.
5.3 e	All new starters who have access to data bearing assets must have their vetting applied for on or before the start of their employment. During this time new starters who are not vetted must be chaperoned until vetting has taken place.
5.3 f	The general facility must have controlled access which will include the following: • No visitors or unauthorised staff will be allowed into data processing areas unless they have their identification verified using photo ID and it is recorded. (NB: This includes drivers, tradesmen and office visitors.) • All visitors and unauthorised staff will always be escorted when in the data processing area.

Highly Desirable

Ref	Criteria
5.3 g	The premises should be operated and occupied solely by the company being certified.
5.3 h	Random staff searches should be in operation.
5.3 i	Staff searches should utilise electronic wands and / or body scanners.
5.3 j	Insider theft should be discouraged by a blend of physical and procedural checks. The following should be used as part of this: • The use of staff lockers in a separate area to the data processing areas. • Restrictions on personal items being allowed within the processing area. • Staff purchase schemes for stock items.
5.3 k	Visitors should wear clearly visible badges and / or vests, which identify them as being non-staff and are always to be escorted in processing areas.

5.4 Process

The chain of custody is imperative to ensure that all assets are controlled within the disposal process. Within the processing facility each stage is reviewed and the risk of failure in process and potential loss of control is assessed. ADISA examines scenarios where a robust process might fail due to unforeseen issues and assesses whether that risk is unacceptable. Review of both written and actual processes is undertaken as well as an assessment of the technology used to perform and manage the process.

5.4.1 Processing

Essential

Ref	Criteria
5.4.1 a	In the absence of a written client specification the maximum length of time from the point of collection until the point of data sanitisation must be 20 working days.
5.4.1 b	Every collection to be processed must be individually tracked within 72 hours of receipt at the facility unless expressly written into a contractual service level agreement (SLA) for client specific requests.
5.4.1 c	In the absence of a written client specification every asset must be audited to obtain a full build specification and create an asset inventory with each asset being uniquely identified.
5.4.1 d	All equipment must undergo de-branding where asset tags and other non-relevant markings are removed.
5.4.1 e	Each device must have the chassis opened to check for unconnected data carrying media such as hard disk drive and full physical checks for other storage devices made (e.g. by opening CD drawers).
5.4.1 f	Any client engagements which require the holding of data carrying assets for longer than the recommended time period must be managed by a written agreement by the service provider and the client, which expressly states that the recommended time has been exceeded at the client's wishes.

Highly Desirable

Ref	Criteria
5.4.1 g	In the absence of a client work specification the maximum length of time from the point of collection until the point of data sanitisation should not exceed five working days.
5.4.1 h	Every collection to be processed should be individually tracked within 24 hours of receipt at the facility unless expressly written into a contractual SLA for client specific requests.

5.4.2 Non ITAD equipment purchases via Brokerage or buy / sell activities.

For the purposes of this criteria the 'non-ITAD' work is viewed as second-hand equipment bought by the ITAD for further selling. Purchases made through legitimate refurbish channels for example, HP Re-Man, are not included in these criteria.

Essential

Ref	Criteria
5.4.2 a	Any equipment bought in as 'non-ITAD' work must have confirmation in writing from the seller that the member has no obligation to sanitise the data.
5.4.2 b	For all non-ITAD work, regardless of 5.4.2 (a), the member must do the following: • Check for digital signature files on a sample of drives. • Ask for certificates of overwriting to accompany the shipment. • Check 10% for data. If data is found in any part of a consignment, all equipment should be processed as an ITAD collection.

Highly Desirable

Ref	Criteria
5.4.2 c	All equipment bought in gets processed as if an ITAD collection.

5.4.3 Segregation

It is imperative that assets which still holds data (pre-processed) and data safe equipment (post process) are segregated throughout the processing activities. This is to ensure any item which still holds data cannot be confused with items which have been processed.

Essential

Ref	Criteria
5.4.3 a	Data carrying assets must be visually segregated from post process equipment. Any opportunity for cross contamination of these assets needs to be marginalised, and where any exists, managed appropriately.

Highly Desirable

Ref	Criteria
5.4.3 b	Data carrying assets should be physically segregated from post process equipment. Any opportunity for cross contamination of these assets needs to be marginalised, and where any exist managed appropriately.
5.4.3 c	Processing streams should be physically managed to ensure that all items are processed in a linear one-way flow once processing is started.

5.5 Software Systems

Records created during the processing of assets need to be safeguarded, so that in the event of a disaster or theft the records can be recovered, and customers can be assured that their data carrying assets were processed correctly.

Essential

Ref	Criteria
5.5 a	Processing database must be backed up monthly.
5.5 b	Back up must be tested once a year.
5.5 c	Back up must be stored off site or in a secure, fire retardant location on site.
5.5 d	Software systems must have a facility, which allows its records to be interrogated and permits recall of items by unique identifier, which stays with the machine.

Highly Desirable

Ref	Criteria
5.5 e	Processing database should be backed up weekly.
5.5 f	Back up should be tested once a quarter.

5.6 Reporting

It is essential for accurate and detailed reporting to be in place in order to help companies using ITAD service providers comply with their regulatory requirements when disposing of data bearing assets. Not only does reporting promote control over the process and therefore help drive excellence, it also demonstrates transparency of the various activities taking place. This openness is essential to help influence perception of the industry and show the number of quality stages inherent to a truly robust IT Asset Disposal process.

Essential

Ref	Criteria
5.6 a	In the absence of a specific client specification the ITAD must provide the client with detailed audit reports to include, but not be limited to: • Serial numbers of devices. • Make. • Model. • Evidence of end point sanitisation.
5.6 b	In addition to (a) the ITAD reports must include copies of the documents used to control the transfer of custody (For example: Collection Notes and / or Waste Transfer Notes) from point of collection through to delivery into processing facility.
5.6 c	The ITAD must provide the client with copies of certificates of destruction and any waste compliance reports.

Highly Desirable

Ref	Criteria
5.6 d	In the absence of a specific written client specification the ITAD should provide the client with detailed audit reports which must include: • Disk drive serial numbers. • Software overwriting report / reference numbers.

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Module 6

Data Sanitisation Capability

Module 6 Data Sanitisation Capability

6.0 Introduction

'Sanitisation' is a term used to describe a process applied to a data carrying media such as tape or magnetic hard drives, which renders the data unrecoverable by a range of forensic techniques. Sanitisation can be achieved by using a piece of software to write data over existing data or by rendering the media itself as no longer operational.

This module assesses each certified ITAD for their capabilities for re-use and destruction against each media type. It not only looks at the toolsets available to the ITAD but also the processes around the use of such toolsets.

ADISA Module 6 Core Principles:

- Understanding data storage media.
- Risk management through data sanitisation processes.
- Quality checks.

6.0.1 Scope

Each certified company will have their capabilities assessed by media type. They are NOT required to process all media types but will only be certified to process those media types for which they, or approved partner, are capable of processing.

Module 6 Data Sanitisation Capability

6.1 Sanitisation Process

These criteria are used to assess the way in which sanitisation tools are used within an ITAD production environment.

Essential

Ref	Criteria
6.1 a	Each ITAD must have all data sanitisation tools identified, verified and published by ADISA in their Data Capability Statement.
6.1 b	In the absence of a client specification, only degaussers from the NSA approved list can be used. All degaussers used must be properly calibrated, have a regular maintenance schedule and a user training programme in place which includes a process for removing all extraneous steel shielding materials (e.g., cabinets, casings, and mounting brackets), but not the hard disk assembly, which must be removed before degaussing.
6.1 c	Any Shredders which are used must have a maintenance schedule (which is to include screen aperture assessment), be designed for use on the media and have a user training programme in place.
6.1 d	In the absence of a written client specification, ALL shredders used must have undergone independent verification of the maximum shred particle size which is to be published as per 6.1 (a).
6.1 e	Software overwriting tools must be configured in a known and documented configuration with regular checks on the configuration to be carried out and documented by staff NOT directly involved in the software usage.
6.1 f	Every data carrying device, which is received for data processing, must undergo the same process regardless of any assurances from the client that they have already destroyed the data.
6.1 g	Any data carrying device which fails must be removed from parent machine, individually tracked via a unique identifier and on-site physical destruction must take place within a controlled and documented process.
6.1 h	Written contingency processes must be in place to deal with instances where equipment fails, where equipment is not supported by the national or internationally approved products being used or when any other external factors impact on the process.

6.2 Quality Control

Essential

Ref	Criteria
6.2 a	There must be a documented quality control process, which will check a sample number of devices per month after the data sanitisation process has been completed. The minimum sample size must be 10 per month of all product types.

Highly Desirable

Ref	Criteria
6.2 b	There should be a documented quality control process, which will check a sample number of devices per month after the data sanitisation process has been completed. The minimum sample size must be 10 per week of all product types.

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Module 7

Waste Management

Module 7 Waste Management

7.0 Introduction

The problem of e-waste dumping is a global issue and whilst ADISA's focus is on the secure sanitisation of data, the issue of exporting of untested electrical equipment is something that ITADs also need to be measured against. This module seeks to offer a basic assessment of a certified company's capability for handling WEEE and/or e-waste. This module does not make reference to any ideological standpoint but looks to check a number of critical elements within each ITAD being assessed.

ADISA Waste Management Core Principles:

- Public statement of permitted WEEE / e-waste capability.
- Full downstream management including auditing.
- Re-use, harvest then recycle.

The Areas of Assessment are:

- Licensing held from regional environmental bodies.
- Treatments being undertaken.
- Public persona and claims in this area.
- Downstream partner management.

7.0.1 Scope

This module is designed to assess the capabilities of an ITAD when receiving items for processing at their own facility. This module applies only to assessing that capability from point of receipt. Please review other modules for elements outside of this scope.

ADISA Module Note

For those companies who hold R2 or e-Steward certifications this module does not need to be complied with.

Module 7 Waste Management

Essential

Ref	Criteria
7.0 a	Each ITAD must have all relevant environmental permits identified, verified and published by ADISA in their Waste Management Capabilities Statement.
7.0 b	Where the company makes collections of waste, the company, or agents acting on its behalf to perform the collection, must hold the relevant permits for the region(s) operated in.
7.0 c	Each collection must have the assets identified as waste or product to identify the right procedures / permits which must be applied for each collection and where the material is waste, whether it is hazardous waste.
7.0 d	The company must not export untreated waste from the country of origin.

Highly Desirable

Ref	Criteria
7.0 e	Where the company receives waste, they should keep records of all incoming movements of material by weight. Protocol weights are permitted.
7.0 f	The company should keep records of all outgoing waste movements by weight.
7.0 g	Where the company receives waste, each site should have personnel in place with suitable levels of qualification.

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Module 8

Product Re-Use

Module 8 Product Re-Use

8.0 Introduction

For many organisations, it is essential that their IT infrastructure comprises the very latest and best technologies to help them maintain a competitive edge. For others, however, a basic functioning device can often be sufficient. This is the reason that ADISA champions the re-use of all assets wherever and whenever possible. By using certified ITADs who deploy verifiable data overwriting software tools, ADISA believes that re-use can become the default position within IT disposal.

Asset re-use carries the twin benefits of maximised revenue opportunity and a positive environmental impact. Legislation is leaning towards encouraging re-use rather than re-cycle, but as the first focus of a client is data security, there is a balance to be achieved between ensuring data is securely sanitised and making processing of the asset financially viable for re-use. ADISA encourages best commercial practice in functionality testing, repair and re-engineering but also recommends considering the commercial viability of these practices.

This module looks at how each ITAD can make products ready for re-use, so that the second (or third) life of the asset offers the user confidence that it has been processed for re-use in the best possible way.

8.0.1 Scope

This module is designed to assess the capabilities of an ITAD when receiving items for processing at their own facility. This module applies only to assessing that capability from point of receipt. Please review other modules for elements outside of this scope.

Module 8 Product Re-Use

Essential

Ref	Criteria
8.0 a	Each asset must be tested to check that it is functional and fit for original purpose.
8.0 b	Each asset must be graded against a written scale to confirm physical condition and records of grading kept with asset record.
8.0 c	Records of all assets either sold on or passed for further processing must be kept. These records must include unique tracking references of all equipment and the destination country. (Destination country must not be a member of any embargoed list.)
8.0 d	All equipment sold to an end user must include a warranty.
8.0 e	Any software installed must hold a legal licence and be the current shipping version unless there is a technical reason for installing an older version.

Highly Desirable

Ref	Criteria
8.0 f	All equipment sold to an end user should include a minimum of a 28 days warranty.
8.0 g	During the auditing process a decision tree should be in place which allows an incomplete or non-functioning asset to undergo some remedial process and / or repair to make it ready for re-use.
8.0 h	Maximum opportunity for re-use of equipment should be in place by the holding of spares, accessories and peripherals to make good damaged, non-functioning or incomplete assets.
8.0 i	All equipment to be re-used should be cosmetically cleaned and where financially viable any missing components must be replaced to ensure maximum opportunity for re-use.

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Module 9

On-Site Services

Module 9 On-Site Services

9.0 Introduction

For many end-users the risk of releasing assets outside of their own control is too great and as such they often wish to conduct data sanitisation services on their own premises. For the purposes of this Standard, 'On-site' means on the client's site.

Due to the very nature of these services, practical assessment of ITAD capability in this area is challenging, as by its nature the service is delivered away from a controlled and auditable environment. In addition, many of the key elements are outside of the ITAD's control, as they are totally dependent on the end-user. As such, ADISA will measure on-site capability by criteria, which are auditable and within the control of the ITAD.

ADISA Module 9 Core Principles:

- Client engagement.
- Process control and data sanitisation.

The Areas of Assessment are:

- Client engagement.
- Range of services.
- Environmental control.
- Processing.
- Reporting.
- Downstream provision.

9.0.1 Scope

This module is designed to assess the capabilities of an ITAD when performing data sanitisation and asset management services on a client site. The core focus is on the control of the working environment, the deployment of the correct tools and the management of the client throughout the engagement.

Module 9 On-Site Services

9.1 Service Provision

It is acknowledged that many clients are unable or reluctant to provide the following information, but it is nonetheless a requirement that evidence of a written request for the following client policy and process is provided (e.g. via a client engagement form).

Essential

Ref	Criteria
9.1 a	All onsite services must be governed by a client engagement process compliant with Module 2.
9.1 b	The use of any sub-processors used must be compliant with Module 3.
9.1 c	There must be a written method for services being undertaken which is to include a risk assessment.
9.1 d	There must be a clearly defined transfer of custody of inventory from client to service provider prior to work commencing.
9.1 e	Prior to work commencing, a site survey must be undertaken. This can be by the completion of a questionnaire and must include security requirements for the processing area and the health and safety considerations for each location.
9.1 f	Quality control procedures and testing samples must be included within the standard process and must be listed within the methodology.
9.1 g	All staff used to perform the service must have undergone specific training in the use of any infrastructure and equipment used during the provision of the service.

Highly Desirable

Ref	Criteria
9.1 h	Prior to work commencing a formal site survey including security requirements for the processing area and health and safety considerations should be carried out for each location.
9.1 i	Prior to work commencing ITAD is to capture high level information about the job to allow for planning and to ensure the correct equipment is taken on site. This is to include: • A unique identifying reference. • Media type within each asset. • Data category of each asset. (If applicable)

9.2 Physical Destruction in vehicle

Essential

Ref	Criteria
9.2 a	Where work is carried out in a vehicle, a designated parking location must be identified for the vehicle.
9.2 b	Where the vehicle is not parked within a controlled parking location there must be a documented risk assessment determining the process for moving assets for destruction from client site to vehicle.
9.2 c	Inventory to be processed must be verified and signed into the control of processor prior to destruction.
9.2 d	The tools for physical destruction must be included in approved Data Capability Statement in Module 6.

Highly Desirable

Ref	Criteria
9.2 e	Where work is carried out in a vehicle there should be internal CCTV to film the drive input process.
9.2 f	Each asset should be scanned / recorded before being processed.
9.2 g	Each asset should be photographed such that the serial number of the device can be viewed before being physically destroyed.

.

Module 9 On-Site Services

9.3 Physical Destruction at client site

Essential

Ref	Criteria
9.3 a	A written site survey must be carried out which is to include location identification, access route and power plan.
9.3 b	A written risk assessment must be carried out which is to include environmental and health implications of operation.
9.3 c	Inventory to be processed must be verified and signed into the control of processor prior to destruction.
9.3 d	The tools for physical destruction must be included in approved Data Capability Statement in Module 6.

Highly Desirable

Ref	Criteria
9.3 e	Each asset should be scanned / recorded before being processed.
9.3 f	Each asset should be photographed such that the serial number of the device can be viewed before being physically destroyed.

9.4 Software overwriting at client site

Essential

Ref	Criteria
9.4 a	There must be a written method statement which denotes how the ITAD will manage the process on client site. This is to include details of how carrying and data safe assets are to be segregated and how cross contamination is to be avoided.
9.4 b	Inventory to be processed must be verified and signed into the control of processor prior to overwriting.
9.4 c	The software and means of deployment must be included in approved Data Capability Statement in Module 6.
9.4 d	Where software overwriting fails, hard drives or data carrying devices must undergo a physical destruction process before being removed from customer site.

9.5 Reporting

Essential

Ref	Criteria
9.5 a	In the absence of a specific client specification the ITAD must provide the client with detailed audit reports to include but not be limited to: • Serial numbers of devices. • Manufacturer. • Model.
9.5 b	The ITAD must provide evidence of the verification and sign-off stages (to include a copy of a sample transfer of custody document).
9.5 c	Client must be provided with evidence of certificates of destruction and any WEEE and/or e-waste compliance reports.

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard 7.0

Module 10

Leasing Process

Module 10 Leasing Organisations

10 Introduction

For leasing companies who wish to achieve certification, Modules 1 through 9 need to be complied with if they perform asset recovery themselves or by their chosen partner. In addition, this module must be included as it assesses how the company manages the lease book into their customers.

ADISA Module 10.0 Core Principles:

- Written Process for Asset Recovery:
  - Policy review.
- Review of asset management capability:
  - Evidence of the ability to track assets into clients and then out is essential.
  - Evidence of the ability to track assets as they are recovered is essential. To include tracking into third party provider and evidence of reporting capability.
- Review of contract(s) in place with service provider(s):
  - Should include full specification for data sanitisation per asset.
  - Should also include service specification. (Such as logistics.)
- Review of your client contracts to show confirmation of data sanitisation service specification.
- Review of website pages pertaining to the asset recovery part of the business.

10.0.1 Scope

This module is designed to assess the capabilities of a leasing company when managing assets into a lessee and then the reverse process out of the lessee into either the direct control of the lessor or their partner.

Module 10 Leasing Process

10.1 Written Process for Asset Recovery

It is essential that all processes undertaken during the asset recovery stage are governed by the leasing company themselves and as such, a review of policy and process control documents is important.

Essential

Ref	Criteria
10.1 a	Review of policy and process documents. These must include: • Full specification for data sanitisation. • Evidence of how the asset is to be controlled throughout the process.

10.2 Review of Asset Management

By the very essence of leasing there is strong and detailed control over assets. The same control must persist after recovery has taken place.

Essential

Ref	Criteria
10.2 a	Organisation must be able to demonstrate the ability to track assets into the lessee and then back out at end of lease term.
10.2 b	Organisation must be able to demonstrate the ability to track assets as they are recovered is essential. To include tracking into third party provider and reporting.

10.3 Partner Management

The use of any third parties for any aspect of the asset recovery process needs to be controlled and managed to ensure performance expectations are met.

Essential

Ref	Criteria
10.3 a	Review of contract(s) in place with service provider(s). • Must include full specification for data sanitisation per asset. • Must include service specification. (Such as logistics.)
10.3 b	Vendor must be selected after a formal and documented selection process.
10.3 c	Vendor must be audited at least once a year.

10.4 Client Engagement

The Data Controller and Data Processor engagement is essential and how the asset recovery service is agreed between the two is an important process. These criteria measure how that relationship is managed.

Essential

Ref	Criteria
10.4 a	There must be a contract in place and that contract should include specific reference to data sanitisation and whether it is part of the agreement between parties.
10.4 b	If a data sanitisation service is offered, then client engagement must be compliant with Module 2.

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ICT Asset Recovery Standard

Appendices

Appendix 1 Supporting Documents available from ADISA

For those companies actively seeking certification then the following documents will be made available as part of the onboarding process. These documents are designed to be generic and will require customising for each applicant. This is done to ensure no attained IP is transferred from one member to another by ADISA. In this regard each applicant should view these documents as guidance to develop your own policies, processes and documentation which can be assessed by ADISA as part of the onboarding process.
This list is subject to change so the current list should be assessed or by contacting ADISA via members@adisa.global.

Supporting Documents for Module 1:

- Your current D and B Risk Indicator Score.
- Confirmation of the correct registration for your region.
- Risk Assessment Template.
- Generic Business Continuity Policy.
- Generic Security Incident Response Plan.
- Copy of Members Code of Conduct.

Supporting Documents for Module 2:

- Generic Data Processing Agreement.

Supporting Documents for Module 3:

- Acting as a Sub-Processor Guidance Notes and ADISA Sub-Processor Form.
- Using a Sub-Processor Guidance Notes and generic Data Processing Agreement.
- Sub-Processor and Third-Party Audit Templates.

Supporting Documents for Module 4:

- Generic Site Survey Template.
- Hub Audit Template.
- Third Party Vehicle Compliance Form.
- Generic Collection Risk Assessment.

Supporting Documents for Module 5:

- Generic Chain of Custody Template.
- Generic Alarm Response Plan.
- Generic Physical Security Check Log.
- Generic Insider Theft Staff Policy and Staff Check Log.

Supporting Documents for Module 6:

- Data Capability Template.
- Degausser Field Output Assessment. (Done at audit – certificate issued).
- Screen Size Verification on Shredders. (Done at audit – certificate issued).
- Generic Quality Control Policy and template to use.

Supporting Documents for Module 8:

- Generic Grading sheet.
- Suggested Testing Processes.

Supporting Documents for Module 9:

- Generic Site Survey Questionnaire.
- Generic Formal Site Survey Template.
- Generic Detailed Site Survey Template.
- Generic Detailed Risk Assessment Template.
- Generic Written Method Statement.

Appendix 2 Dun and Bradstreet Risk Indicator

Supporting Documentation

Module 1: Business Credentials – Dun and Bradstreet Risk Indicator

The Condition Code or Risk Indicator

This is calculated by taking into account key items within the Business Information report, which are used to predict the likelihood of a business failure.

Risk Indicator	Probability of failure	Guide to interpretation
1	Minimal risk	Proceed with transaction – offer terms required
2	Low risk	Proceed with transaction
3	Greater than average risk	Proceed with transaction but monitor closely
4	Significant level of risk	Take suitable assurances before extending credit
5	Insufficient information to assign a risk indicator	No public information or Dun and Bradstreet proprietary information available to indicate trading activity

The Risk Indicator in more detail:

- Strong Condition (1)
  This is assigned to companies of undoubted credit standing and financial strength. The risk associated with being a creditor of these concerns would be negligible or zero, the concern which pays bills promptly or discount.
- Good Condition (2)
  This is assigned to financially sound concerns, having no known record of bad payments and paying suppliers quickly. The risk of being associated with being a creditor of these concerns would be low and they would be classified as an ordinary trade risk.
- Fair Condition (3)
  This would be assigned to concerns believed to be financially sound but with a history of slow payments or some losses or working capital deficit. The risk associated with being a creditor of these concerns is higher and would be classified as potentially slow payers or fair-trade risk.
- Poor Condition (4)
  This would be assigned to concerns of known financial weakness. A number of years' losses, higher than normal working capital deficit, a negative tangible net worth which is worsening, court judgments, bad payments etc. This risk is associated with being a creditor of these concerns is high or significant.
- Undetermined (5)
  This is assigned to concerns where there is insufficient information available to express any opinion on the condition, financial soundness or payment history of the concern.

Source: Dun and Bradstreet

Asset Disposal and Information Security Alliance Limited

EMEA Phone: + 44 845 557 7726
US Phone: +1 832 696 0787

Registered Office
31 Thrales End Business Centre, Thrales End Lane, Harpenden, AL5 3NS, United Kingdom

www.adisa.global
info@adisa.global