ADISA

ASSET DISPOSAL & INFORMATION
SECURITY ALLIANCE

ADISA Claims Test Service.

Version	1.0
Status	Released
Date	07/01/2014
Author	Professor Andrew Blyth and Steve Mellings
Review Date	18th December 2014

Contents.

1.0 Conceptual Introduction to Information Security.

Information Security is concerned with the protection of assets from various threats, where an asset is an entity that someone places value upon. Examples of an asset can be a physical asset such as a hard drive, a logical asset such as data or software. Figure 1 illustrates these high-level concepts and relationships.

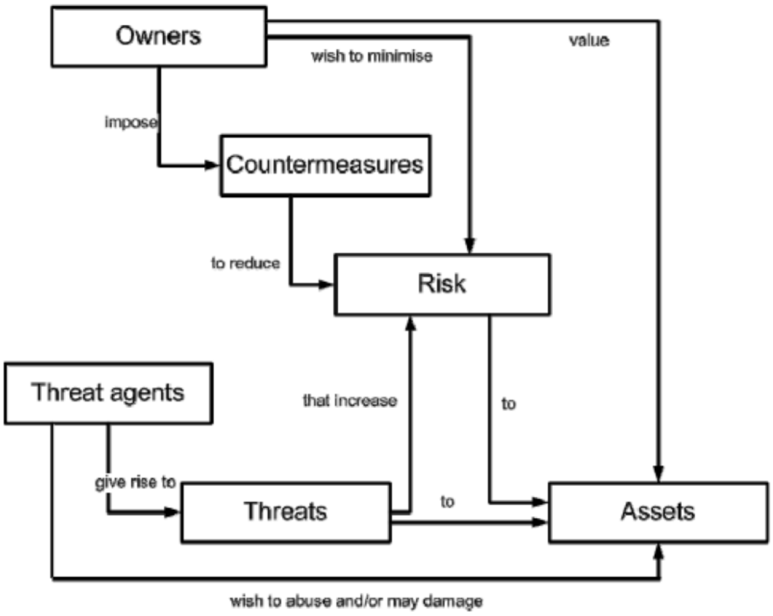


Figure 1 – Security concepts and relationships

Safeguarding assets of interest is the responsibility of owners who place value on those assets. Threat agents may also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner. Examples of threat agents include hackers, malicious users, non-malicious users, computer processes and accidents.

The owners of the assets will perceive such threats as potential for impairment of the assets such that the value of the assets to the owners would be reduced. Examples of security-specific impairment commonly include, but are not limited to: loss of asset confidentiality, loss of asset integrity and loss of asset availability.

These threats therefore give rise to risks to the assets, based on the likelihood of a threat being realized and the impact on the assets when that threat is carried out. Subsequently countermeasures are imposed to reduce the risks to assets. These countermeasures may consist of IT countermeasures and non-IT countermeasures.

Owners of assets may be (held) responsible under a regulatory framework, such as the Data Protection Act 1998, for those assets and therefore should be able to defend the decision to accept the risks of exposing the assets to the threats. Two important elements in defending this decision are being able to demonstrate that:

- The countermeasures are sufficient: if the countermeasures do what they claim to do, the threats to the assets are countered;
- The countermeasures are correct: the countermeasures do what they claim to do.

Many owners of assets lack the knowledge, expertise or resources necessary to judge sufficiency and correctness of the countermeasures, and they may not wish to rely solely on the assertions of the developers of the countermeasures. These asset owners may therefore choose to increase their confidence in the sufficiency and correctness of some or all of their countermeasures by ordering an evaluation of these countermeasures.

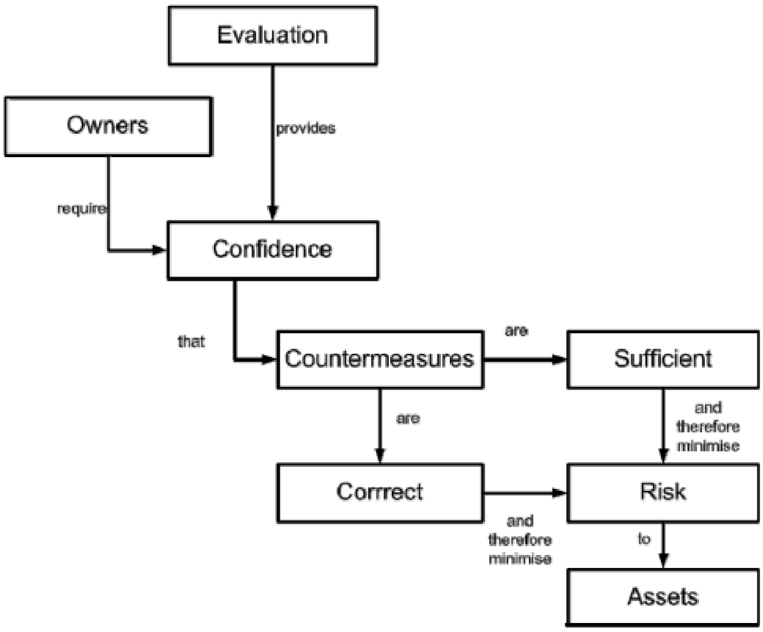


Figure 2 – Evaluation and its Concepts

Owners of an asset may seek to utilize a countermeasure to mitigate a specific threat from a threat agent. In utilizing this countermeasure the owners of the asset need to assure themselves that the countermeasure is correct and fit for purpose. In short, they need to have confidence that when a product vendor makes a claim, that the claim has been tested and certified by an independent authority.

2.0 Threat Capability Assessment.

Within this method the test levels are based on the technical capabilities of defined potential threat actors. The ADISA approach to verifying the viability of products for use as data sanitisation tools is risk based. The term risk is defined as follows from ISO 13335/1/2004.

> "*A risk is a potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation. It is measured in terms of a combination of the probability of an event and its consequence*."

2.1 The Threat Matrix.

The threat matrix defines a series of capabilities and risks that various threat agents can pose against an asset. The test levels define a series of capabilities that a threat actor/agent may wish to bring against an asset either by direct access to the asset or access via its location within a device.

ADISA Risk Level	Threat Actor and Compromise Methods	Type of Method	ADISA Test Level
1 (Very Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilising freeware, and OS tools.	Keyboard attacks from a motivated individual. Typical attack could be using open-source forensic tools.	1
2 (Low)	Commercial data recovery organisation able to mount ADISA Risk Level 1 attacks and non-invasive and non-destructive COTS software attacks and hardware attacks.	Keyboard attacks from a motivated professional organisation. Typical attack could be using commercial tools.	1
3 (Medium)	Commercial computer forensics organisation able to mount ADISA Risk Level 2 attacks and invasive/non-destructive software and hardware attack, utilising COTS products.	Laboratory attacks from commercial data recovery experts. Typical attack could be: Chip Readers/bus decoders.	2
4 (High)	Commercial data recovery and computer forensics organisation able to mount ADISA Risk Level 3 attacks and invasive/destructive software and hardware attack, utilising both COTS and bespoke utilities.	Laboratory attacks from specialist forensic scientists. Typical attack would involve analysis of individual hardware components.	2
5 (Very High)	Government-sponsored organisations using advanced techniques to mount all types of software and hardware attacks with unlimited time and resources to recover sanitised data.	An attack agent of unknown capability and unlimited resource. Typical attacks: Taking theoretical forensic possibilities and making them an actual capability.	3

Table 1 – The Threat Matrix

When making a claim for a product, which sanitises data and therefore renders the data unrecoverable, a relationship must be defined between the claim and the level of risk that the claim is designed to mitigate.

2.2 Explanation of risk levels.

The risk levels utilised within this document are based on ADISA’s own risk assessment methodology (See Appendix B). Acceptance of the method outlined in this document is dependent on the data controller/end user assessing whether their own risk assessment is comparable to the ADISA risk assessment in this field.

3.0 Scheme Introduction.

In conjunction with the University of South Wales, the ADISA Claims Test Scheme (ACTS) is designed to offer manufacturers of products, which are designed to sanitise data, an independent validation scheme to confirm the claims made about their products.

There are five families of products, which can be tested under this scheme:

1 – Software overwriting solutions for both magnetic hard drives. (HDD)
2 – Software overwriting solutions for solid state drives. (SSD)
3 – Software overwriting solutions for smart phones utilising SSD technology.
4 – Hardware destruction tools.
5 – Hardware shredding tools.

Each claims test follows the same methodology, which is outlined in this document.

3.1 Objectives of ACTS.

The objective of ACTS:

- Verify manufacturer's product claims are accurate.
- To provide an independent platform to assist manufacturers in the positioning of their products within the security market place.
- Help users of the products tested to have more information from which to make risk based decisions on the acceptable usage of such products for data sanitisation purposes.

3.2 Scheme Stakeholders.

There are three groups with a general interest in evaluation of the countermeasure/claim: consumers, developers and evaluators. The criterion presented in this methodology has been structured to support the needs of all three groups. They are all considered to be the principal users of the ADISA claims test scheme (ACTS).

3.2.1 Consumer

ACTS is written to ensure that evaluation fulfills the needs of the consumers, as this is the fundamental purpose and justification for the evaluation process. Consumers can use the results of evaluations to help decide whether a countermeasure/claim fulfills their security needs. These security needs are typically identified as a result of both risk analysis and policy direction. Consumers can also use the evaluation results to compare different claims.

3.2.2 Developers

ACTS is intended to support developers in preparing for, and assisting in the evaluation, of their products claim. ACTS can be used to determine the responsibilities and actions to provide evidence that is necessary to support the evaluation of the products claim.

3.2.3 Evaluators

ACTS contains criteria to be used by evaluators when forming judgments about the conformance and performance of a developers products claim.

3.3 Exclusions from ACT scheme.

Should a claim be made which is insufficient in the eyes of the testing authority for a product to be classed as fit for purpose, the claim will be rejected.

Products that are approved under ACTS are done so based on a commercial environment. For companies processing government data they should refer to the approved schemes by their respective governments.

4.0 ACT Project Plan.

4.1 Constructing a claim.

The key element of ACTS is the claim itself. Claims can be constructed in one of two ways:

1 – Free Form Claim.

This is where the claimant writes a specific claim about their product. This can be made up of any element and any form of deployment. These claims are the most difficult to get accepted as they must be prescriptive, absolute and measurable and the claimant is encouraged to seek assistance before submitting such claims.

2 – Structured Claim.

To ensure a consistent approach to claims testing, ADISA and the University of South Wales have a generic claims statement. This statement has four stages; Product Introduction, Claim, Risk Level and technical requirements.

- Product Introduction
  - The name and revision of the product must be listed. If only part of a product is to be tested then that must also be listed. If the product or software has configurable options, which are all bundled within one revision type then the chosen configuration for testing must be listed or ALL configurations are required to be tested.
- Claim
  - The objective of the claim section is to provide a clear and unambiguous statement of the claim being made. Reference should be made to how the product is deployed/used, and on what media it is to be used.
- Risk Level
  - With reference to the ADISA Threat Matrix (2.1 Table 1) please identify the risk level that the product can be used to protect against.
- Technical Requirements
  - Hardware and software platforms required to make the countermeasures function correctly.
  - The policy and procedures to make the countermeasures function correctly.
  - Guidelines governing the correct usage of the claim (countermeasure) so as to mitigate the defined threat.

4.2 Provision of hardware/software required for testing.

Each claimant will be responsible for supplying the relevant hardware/software against which the claim is made. The testing laboratory will be responsible for purchasing relevant hardware on which to test the claim. This hardware cost will be passed on to the test claimant and the hardware will be consumed during testing.

Specific details will be agreed for each test made.

5.0 Claims Test Process.

Upon successful acceptance of the claims document and provision of the required hardware/software to execute the claim the test process for each type of claim will be executed as per the high level overview below. Sample size for each test will be sufficient to ensure test anomalies are removed from the report.

5.1 Software overwriting solutions for magnetic hard drives. (HDD)

Phase 1: Known data is written to every logical block address of the drive including areas such as HPA and DCO.
Phase 2: The claim subject is executed on the device in accordance with the manufacturer’s guidelines.
Phase 3: The device is then put through a forensic process in accordance with the capabilities of the risk level being tested against.
Phase 4: The results are analyzed.
Phase 5: The report is produced and issued to test claimant.

5.2 Software overwriting solutions for solid state drives. (SSD)

Phase 1: Known data is written to every logical block address of the drive.
Phase 2: The claim subject is executed on the device in accordance with the manufacturer’s guidelines.
Phase 3: The device is then put through a forensic process in accordance with the capabilities of the risk level being tested against.
Phase 4: The results are analyzed.
Phase 5: The report is produced and issued to test claimant.

5.3 Software overwriting solutions for smart phones utilizing SSD technology.

Phase 1: Smart phone being tested is put into a stable known condition by in accordance with the manufacturer’s guidelines.
Phase 2: Known data is written to the device.
Phase 3: The claim subject is executed on the device in accordance with the manufacturer’s guidelines.
Phase 4: The device is then put through a forensic process in accordance with the capabilities of the risk level being tested against.
Phase 5: The results are analyzed.
Phase 6: The report is produced and issued to test claimant.

5.4 Hardware destruction tools.

Phase 1: Known data is written to the media against which the claim in made.
Phase 2: The claim subject is executed on the media in accordance with the manufacturer’s guidelines.
Phase 3: The media is then put through a forensic process in accordance with the capabilities of the risk level being tested against.
Phase 4: The results are analyzed.
Phase 5: The report is produced and issued to test claimant.

5.5 Hardware shredding tools.

Phase 1: Known data is written to the media against which the claim is made.
Phase 2: The media undergoes shredding in accordance with the manufacturers guidelines.
Phase 3: The shred particulate is recovered and the longest and the shortest dimensions of the shred particulate are recorded.
Phase 4: The report is produced and issued to test claimant.

Statement on Shred Claims: Manufacturers of shredders sell their products based on the thickness of the blades/knives. A sieve is then used by the operators to manage a consistent output from the shredder. The size of the hole in the sieve is commonly used to classify the size of the shred particulate but this is incorrect. For example, 20mm x 3mm x 4mm particulate will fit through a 5mm x 5mm sieve. As such the report will include a volume measurement from the largest particulate in the sample size and will list the dimensions of this particulate.

6.0 Glossary.

ADISA	Asset Disposal and Information Assurance Alliance.
COTS	Commercial off the shelf software.
CPA	Claims Product Assurance.
Destructive	A test which when performed renders the device unfit for purpose.
Invasive	A test which is performed by physical intrusion into the device.
LBA	Logical Block Address.
Non-destructive	A test which performed which leaves the device fit for purpose.
Non-invasive	A test which does not physically intrude into the device.
OS	Operating System.
SSD	Solid State Storage Device.

Appendix A – Example of a Claims Testing Application Form

Form Number ADPC _______

Section 1 – Applicant Information

Company Name ____

Address ____

____

General Contact

Name ______________________

Phone ______________________

Mobile ______________________

E-mail ______________________

Section 2 – The Claim Target (See 4.2 for guidance on completing)

____

____

____

____

____

____

____

____

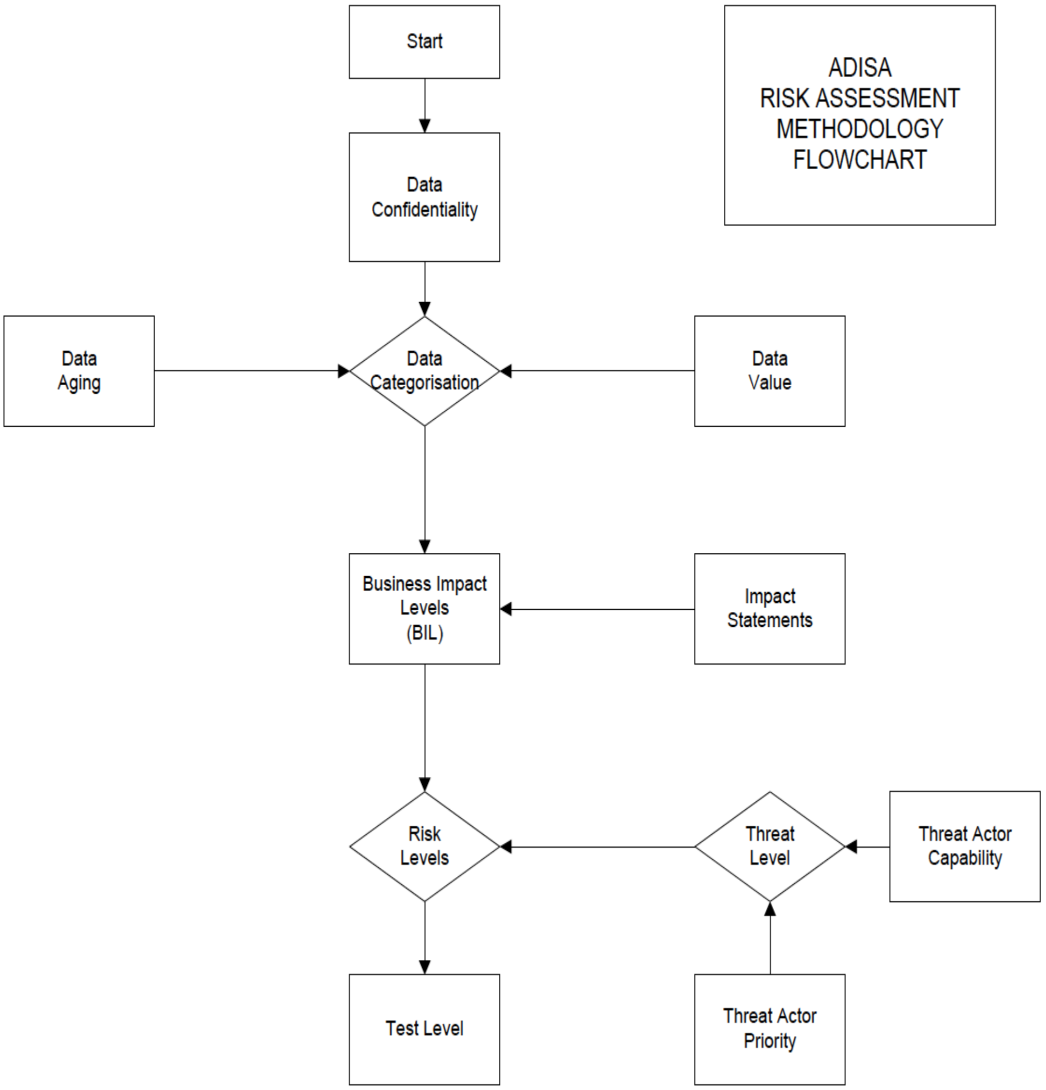
I [Claim Applicant Name] of [Claims Applicant Company] confirm that the information outlined in this document is an accurate and true reflection of the claims made by our product wishing to undergo the ADISA testing method.

Signed on behalf of {Claims Applicant Company}
SIGNED: ______________________
NAME: ______________________
TITLE: ______________________
DATE: ______________________
Claim Accepted by:

Signed on behalf of University of South Wales
SIGNED: ________________
NAME: ______________________
TITLE: ______________________
DATE: ______________________

Signed on behalf of ADISA
SIGNED: ________________
NAME: ______________________
TITLE: ______________________
DATE: ______________________

Appendix B – ADISA Risk Assessment Methodology


Start
ADISA RISK ASSESSMENT METHODOLOGY FLOWCHART
Data Confidentiality
Data Aging
Data Categorisation
Data Value
Business Impact Levels (BIL)
Impact Statements
Risk Levels
Threat Level
Threat Actor Capability
Test Level
Threat Actor Priority