

#becrypt

Protecting Valuable Data and Managing Information Risk

Becrypt Guide to Information Assurance

Introduction

All organisations, whether in the public or private sector face the challenge of protecting valuable corporate and personal data. Indeed they are required to protect personal data by law, under the Data Protection Act and even the Human Rights Act. While in Central Government there has long been a culture of protecting secrets, many organisations outside of Central Government might feel that they did not deal in such secret data, and so had no need to worry.

However, many data loss incidents in recent years have alerted us to the toxic liability of holding data. If lost or leaked, it can wreck an otherwise spotless reputation, it can cause financial loss due to lost contracts, or commercial secrets leaked to competitors. It can result in identity theft for individuals and fraud. On top of all this, organisations can be subject to hefty fines from regulatory bodies.

This guide explains what Information Assurance (IA) is, and how it can be applied to your organisation to protect data, and avoid the risks associated with its loss or leakage.

The Guide has been design to cover all of the key areas an IT Security Professional would need to consider when creating an IA strategy and implementing an effective IA policy across their organisation.

At the heart of the Guide is the belief that technology alone can not solve the problem of Information protection. It is very much a people, process and technology conundrum. Organisations need to take a wider view of information protection and formulate a sound Information Assurance strategy encompassing people and processes combined with the use of the right technology.

The Guide starts with an explanation of what IA is and how it can be applied to your organisation and goes on to address the principals of compliance, the Whole Life Assurance Mode, risk mitigation models, 'people, places, policy and procedure' as well as Technical Data Security.

Also included in the Appendices are useful templates:

- IT Staff training Programme Syllabus, addresses the important elements IT Staff need to understanding when implementing IA policy, such as identifying sensitive data, understanding security levels for Data and setting IT security policy.
- Writing an effective data security policy, covers all of the points you need to consider when writing and documenting a security policy, such as setting security goals and identifying what to protect through to physical security and policy for Removable Media.

What is Information Assurance

IA is the practice of managing information-related risks. It protects information and information systems by ensuring confidentiality, integrity, availability, authentication and non-repudiation.

This applies to information whether it is held in storage, processing, or in transit, and covers both malicious and accidental threats.

Information Assurance is a further development of Information Security. IA has a broader remit as it includes risk management as well as the tools used to protect data. IA also covers such issues as corporate governance, privacy laws, data protection laws, compliance, business continuity and disaster recovery.

Confidentiality

Data confidentiality is about ensuring that only those authorised have access to the data. Typically, information should have a confidentiality level (in the UK government there are seven impact levels from 0 to 6, covering, Not Protectively Marked, Protect, Restricted, Confidential, Secret, Top Secret). Data aggregation can increase the confidentiality level of data. For instance, name and address details may be one level of confidentiality, but when paired up with bank account details, this should become a far higher level of confidentiality because the data is more sensitive and more valuable, and potentially more damaging if lost or compromised.

Integrity

Integrity is about protecting the data and ensuring that it has not been tampered with. This means data can not be created, changed, or deleted without proper authorisation. It also means that data stored in one part of a database is in agreement with other related data stored elsewhere.

The unintended modification or loss of data is the most prominent cause of loss of integrity. This could be through human error, hardware or software errors, or through physical causes such as floods or fire.

Intentionally altering data is potentially the most dangerous risk for data integrity. Malicious codes such as viruses and worms have the capability to corrupt the data.

Authenticity

Authenticity is necessary to ensure that the users, documents and data are who or what they say they are.

Availability

Availability means that the information and the systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is needed. Availability also means that people authorised are able to access the information when they need to.

Non-repudiation

Non-repudiation means that one party of a transaction can not deny having received a transaction nor can the other party deny having sent a transaction.

Principals of Compliance

Risk Management

Risk can be defined as the combination of the probability of an event and its consequences. Risk management is a central part of any organisation's Information Assurance strategy. It is the process whereby the organisation methodically addresses the risks attached to the storing and use of data with the goal of avoiding the bad outcomes should data be lost, exposed or misused in anyway. Part of the risk management equation is to balance the amount of resource allocated to avoiding the bad outcome, so that the avoidance does not become more of a burden than the outcome itself.

Risk management identifies, assesses and prioritises risks, then coordinates an economical application of resources to minimise, monitor, and control the probability and/or impact of bad outcomes. Risks with the highest probability of occurring and the greatest loss should be tackled first.

Risk Mitigation

Risk mitigation is the process of applying additional controls (whether that be personnel, procedural, physical or technical) to reduce the severity or likelihood of the risk from occurring. For example, using encryption to protect data on a laptop ensures that if the laptop is lost or stolen, the data is inaccessible without the correct password. The laptop is still lost and will have to be replaced, but at least the data is safe because no-one can read it.

Whole of Life Assurance Model

It is important that while information is protected, it is still easy for authorised recipients to access it. Information that leaves direct control must be protected by clear processes which ensure that the right person is authorised to receive and access it.

The Whole of Life Assurance Model is for anyone that manages the technical risks to information assets or data. The model can be used to identify alternative ways of mitigating the impact or likelihood of a risk. It comprises of four elements:

- Those considerations associated with the concept, origin and development of an ICT solution (Intrinsic)
- Those considerations associated with the independent testing of an ICT solution outside the development environment (Extrinsic)
- Those considerations associated with the architecture of the ICT solution and its integration with the business (Implementation)
- Those considerations associated with an ICT solution that handles 'live' information or that is used or relied on by the business (Operational)

By considering the mitigations for a risk across all of these elements, the risk managers or owners can build up a whole-life risk management plan. They can choose the most appropriate approach to managing an information risk, balancing the needs of the business for functionality, with the need to manage the risks to the integrity, availability and confidentiality of its data.

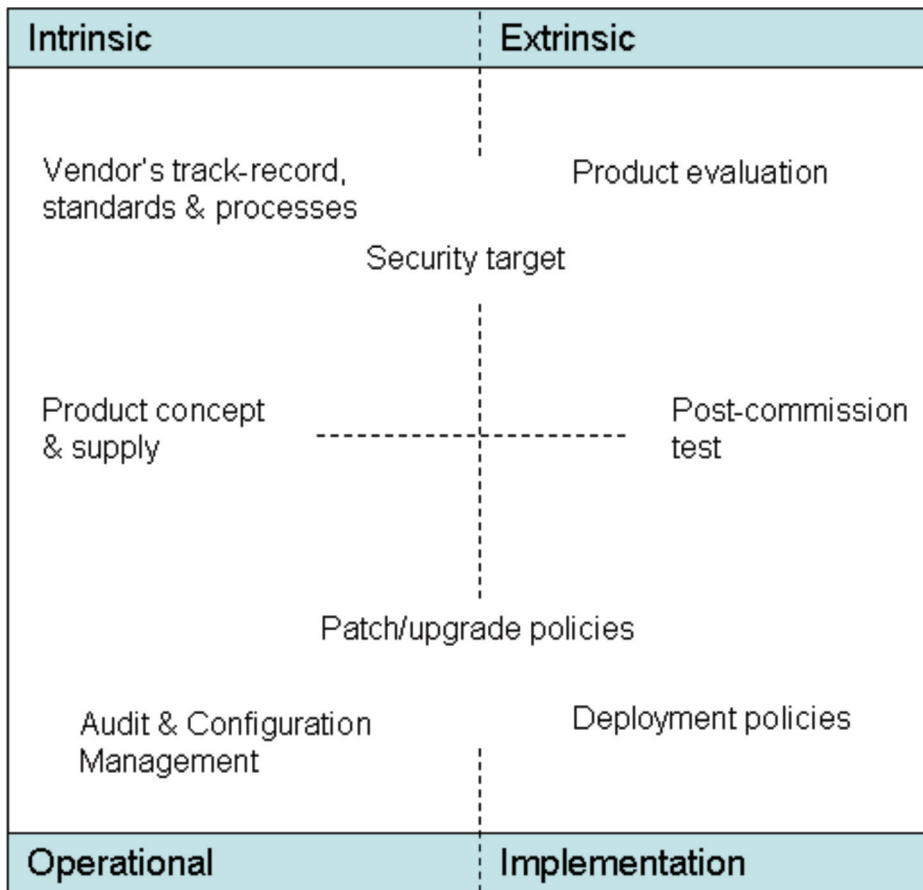
An example of this framework might be used with a firewall. A firewall controls access across an IT network boundary and its policies must reflect the needs of the business. A risk assessment of a network connection might determine that an assured product is needed.

However, using the Assurance Model a risk manager may additionally ask the following questions;

- How much trust will be needed in the supply chain, both now and later? (Intrinsic, Operational)
- How will upgrades or patching be performed? (Intrinsic, Operational)
- Does the hardware or software need to be evaluated to mitigate the risks, or would regular penetration testing be more appropriate? (Extrinsic, Operational)
- Will the firewall be integrated into the business so its security functions are not degraded? (Implementation)
- Can the firewall be configured to support the access policies that the business needs? (Intrinsic, Implementation)
- How will illicit access attempts be identified and what will be done if they occur? (Implementation, Operational)

Such questions can be asked at any point in the solution life-cycle, but are most powerful when asked continuously.

Examples of risk management by category



People and Places, Policy and Procedure

After several well documented data losses, Central Government are now working hard to effect a change in culture to one where personal data is viewed as a valuable asset and treated with the utmost respect. Other public sector organisations and those in the commercial sector need to follow this lead. This culture change has to be adopted from the top and driven down throughout the organisation. It starts with people and is reflected in policies and finally into the procedures that people follow.

As organisations develop a culture that understands the value of information and data as a key business asset, it becomes clear that it is not just an IT issue. There should be clear lines of accountability throughout the organisation with continuous staff education and awareness programmes.

People and Places

All organisations should appoint a Senior Information Risk Owner (SIRO). This person should be a senior manager that understands information risk and should be able to provide advice and guidance to the organisation about how to set and run its IA policies and procedures.

IT systems should be assigned an Information Asset Owner who is a business manager operationally involved with the system and the data it contains. This person has the day-to-day understanding of how the information is held, how it is accessed, who has access to it and why. The Information Asset Owner understands the level of business risk associated with the system and ensures that the system operates within acceptable levels of risk. The Information Asset Owner regularly reviews user access rights covering staff, contractors and suppliers.

Reporting procedures should be put in place to manage any information risk incidents. As well as standard audit trails and alerts when there is a security breach, this should also include mechanisms to allow any employee to bring to the attention of senior management any concerns about information security.

Regular risk assessments should be conducted to ensure that systems are kept secure, and that procedures are followed. These should cover all elements of security including confidentiality, integrity, availability, authentication and non-repudiation. Security of information held can be compromised by the physical

security of the building where it is held or accessed. It is equally important to assess the physical security of buildings and the layout of offices. People should not be accessing sensitive data, for example, in open plan offices, where they can be overlooked. Physical security should also be assessed regularly, ensuring that all staff have ID cards which are worn, and people without visible ID are challenged. Visitors to buildings should be recorded and accompanied at all times.

Clear desk and clear screen policies should be implemented to ensure that sensitive information is not seen by unauthorised people and any printed material should be locked away when not in use.

At the end of its life sensitive information should be disposed of securely. Electronic files should be overwritten, erased or degaussed. Paper records should be shredded, pulped or incinerated. Wherever possible the use of removable media to store data should be avoided, but where it is necessary appropriate security, such as encryption and password protection, should be put in place. The use of removable media devices themselves should also be further controlled via a port control system.

Policy

Every organisation should have documented security policies. These should be communicated to staff as well as suppliers and contractors. When suppliers and contractors handle information it is important that they adhere to the same documented policies and standards. Security policies should work on the premise of giving people the minimum access to data so that they can do their job or complete their task, and no more.

Personal and sensitive information should be kept within secure premises and within secure systems and wherever possible access should be limited to within these secure premises. However, where this is not possible, or it is desirable to give someone remote access (for instance giving access to mobile/home workers – this is a risk management decision), it should be via a secure connection where information can only be viewed or amended.

Ideally data should not be able to be stored on the remote computer, but where it is, it should be downloaded via a secure connection, and the computer itself subject to security assessment (data should be encrypted and password protected at the very least). Bulk transfer of data should only be carried out via a secure network and never via normal email systems.

Independent specialists that are suitably qualified and registered (members of TigerScheme, Crest or CHECK) should be engaged to carry out regular penetration testing.

Procedure

Every organisation should set out in a policy document the procedures for dealing with all aspects of Information Security and how to implement them.

The policy should also include procedures for recovering from a data security incident, which will document what measures, should be taken in the event of a major data breach. A complete security risk plan should be completed at least once a year to ensure that all threats are being addressed and that current procedures are still being adhered to. All policies and procedures should be tested regularly.

The primary tool for assessing an information system and providing procedural guidance to users is an IA Risk Management document.

The IA Risk Management template is available on request. Please email ia@becrypt.com or call us on 0845 838 2080.

The template for Writing a Data Security Policy is available in the Appendix - Template A

Technical Data Security

Data Handling

It is crucial to understand the importance of your data assets. Data classification enables organisations to store data in line with compliance controls. It also enables organisations to store data in the most effective manner. A data classification process should be completed so that it is possible to see clearly how different types of data should be treated. Not only will it become evident which data is sensitive and therefore needs to be protected, it will also be a useful exercise for business intelligence. Classifying information according to business criteria has multiple impact points including security, archiving, retention and destruction. Therefore any such exercise will necessarily involve business units as well as IT, compliance and legal.

Many data classification projects fail because they aim too high and are overly complex. The key to success is to keep it simple and not have too many classes or levels. In a multi-level system where each asset has a label, if there are too many levels you can end up with more metadata than data.

For most organisations five security levels should be adequate. Each level should have appropriate technical and procedural models assigned. To keep things simple it may be possible to apply set procedures at department or business unit level, or by applications. For instance, it is far simpler to encrypt every laptop in your organisation than ask each user what data they hold on the laptop and how it is used.

One of the largest challenges to a successful data classification project is educating users, particularly where they are not used to thinking about data security. This is another reason for keeping things as simple as possible.

Data protection strategy

One of the most important reasons for creating a security policy, apart from the fact that data assets must be protected, is to ensure that efforts spent on security yield cost effective benefits. Basic steps for creating a data protection strategy are:

- Identify what information you are trying to protect; i.e. personal data, valuable proprietary information, intellectual property and if you have dealings with government or public sector, governmental or sensitive information
- Determine what you are protecting it from; i.e. unauthorised access to the information, unintended and/or unauthorised disclosure of information and denial of service
- Determine how likely the threats are; it is far more likely that someone will lose a laptop or a USB stick than your office be subject to a break in
- Implement measures which will protect your assets in a cost-effective way
- Review the process continuously and make improvements each time a weakness is found

The IA Risk Management document can help to formulate the strategy.

Security operation procedures (SyOPs)

Staff can not be expected to instinctively know about data security. Creating procedural policy, i.e. what staff can and can't do is key to communicating with staff, educating them and ensuring that they are aware of their data security responsibilities. Areas to consider are:

1. Securing data assets. Ensure that data is held within a secure system, protected by passwords, maybe strengthened with two factor authentication and encryption. Where data assets are in transit ensure that a secure method is used, either secure network with secure, authenticated end points or an encrypted removable media device.
2. Restricting assets. Ensure access is given only to those people that need it to do their job. Use passwords and authentication to ensure the person is who they say they are. Maintain an access rights database, with systems which access can be authorised against (if required).
3. Strong password protection. Ensure that strict guidelines are published for password generation. They should be changed at least every 90 days, and immediately if there is any reason to suspect that the password has been compromised. Real words should not be used (peoples/pets names etc). Passwords should include a mix of upper and lower case letters, numbers and symbols.
4. Patching policy. This is covered within the IA Risk Management document and should be built into the change management processes within the company. Each time a change is made documentation should be updated immediately and staff alerted.

5. Malware / virus checks. Systems should be set up to automatically check for malware. For instance firewalls, spam filters, and virus checkers on individual PCs. Any system should be set to automatically look for malware whenever any new data is introduced, and the connection of any external device to the network or an individual PC should also generate an automatic virus scan of the device. Automation is the key here, wherever possible it should never be left to individuals to remember to check for malware.
6. Data back-up/storage. Systems should be set to automatically back-up data to a secure area. When stored data should be clearly labelled by its security level so that it is obvious where and how it should be stored. Data handling procedures should be associated with each data security level.

Personnel Vetting

There is a great deal of publicity about intruders and external threats to systems, but most surveys show that for most organisations the actual loss from insiders is much greater. It is therefore important to know who has access to data. This should start with appropriate background checks of potential employees and those that will handle sensitive data. Vetting can take several forms, the employer may simply follow up on previous employers references, or an external agency may provide the vetting service which can include criminal record disclosure and cyber-vetting. In any situation, any form of vetting needs to be carried out sensitively (particularly when it concerns current employees) and the person being vetted must be informed.

Physical location – GSE, LSE, ESE (SE stands for secure operating environment)

Audit and accounting for data assets

Data assets should be audited at least on an annual basis, ideally by an external agency that specialises in such work. Details of all data assets should be held on an asset register where the security level is also recorded. Each asset or system should be assigned an owner, ideally from the business that has an understanding of the data asset and how it is used.

Training and awareness

Communicating security policies and procedures to employees, and getting their commitment to adopting them is an important part of lowering risk of data loss or leakage. Basic training in the principles of data security should be mandatory for all staff. Staff that work with data need to know how to use the systems in a security conscious way. Areas to consider include:

- Training staff to use systems correctly
- Communicate data security procedures and principles, including getting signed declarations from anyone handling sensitive data
- Set out good IT practice covering email, the internet, business applications and bringing personal devices and applications into the workplace
- Include data security responsibilities within staff contracts
- Involve staff in risk assessments and regular reviews and audits of systems and procedures

The template for Data Security Staff Training is available in the Appendix - Template B

In Summary

Organisations need to have a clear understanding of the following points:

- What data is held, where it is kept, who has access to it and where it goes to
- The business impact should any of that data be lost, stolen, or compromised
- The principles of Information Security, Information Assurance and Risk Management and how to apply them
- What and who specifically the data needs to be protected from – usually uncovered by Risk Assessment

Having identified the data and associated risks organisations should undertake the following actions:

- Appoint a Senior Information Risk Owner (SIRO) who will provide help and guidance in setting up organisation wide IA policies and procedures
- Assign Information Asset Owners to each business system who is operationally involved with the system and the data it contains
- Set up documented policies and procedures for IA which include detailed instructions for handling data, reviewed and updated each time the system changes
- Address the technical aspects of protecting data, using appropriate tools/technology. For example,
 - Encrypting data held on portable devices like laptops, PDAs and removable media such as USB sticks, and CDs/DVDs.
 - Control the flow of data into and out of the organisation using End point control/port control solutions

- Ensuring that mobile/home workers have secure access to corporate systems and data, and limiting their access as appropriate
- Enforcing the use of strong passwords
- Introducing two factor authentication where appropriate
- Ensuring automated procedures for updating anti-virus, anti-malware, firewalls, and patching
- Ensuring data is backed up and stored securely
- Identifying how data will be disposed of at the end of its life
- Address location issues, for instance, staff viewing sensitive data in public places or where they can be overlooked by unauthorised staff.
- Consider vetting staff that will handle sensitive data
- Set up audit trails of when, how and by whom data is accessed, with alerts for non-compliant actions
- Set up training and education programmes for staff, with refresher courses where possible.
- Appoint a suitably qualified independent specialist to audit IA systems to ensure they are adequate and provide penetration testing.
- Conduct a system audit at least annually.

Becrypt's Information Assurance Risk Management Document gives a full template for implementing, running and decommissioning an Information Security system.

To request a copy, please email ia@becrypt.com or call us on 0845 838 2080.

For further reading the following websites may provide useful information.

Useful Links

Information Assurance Advisory Council <http://www.iaac.org.uk/>

CESG – the National Technical Authority for Information Assurance http://www.cesg.gov.uk/about_us/index.shtml

Cabinet Office, Central Sponsor for Information Assurance <http://www.cabinetoffice.gov.uk/csia.aspx>

HMG Baseline Personnel Security Standard http://www.cabinetoffice.gov.uk/media/45160/hmg_bpss.pdf

BCS – British Computer Society <http://www.bcs.org/server.php?show=nav.8256>

SOCITM – Society of Information Management <http://www.socitm.gov.uk/socitm/Transformation/Information+Assurance/default.htm>

Get Safe Online – Practical advice www.getsafeonline.org/

Council of Registered Ethical Security Testers
<http://www.crest-approved.org/>

TigerScheme, independently certifying the skills of vulnerability test (penetration test) engineers. <http://www.tigerscheme.org/>

CHECK, IT Health Check service run by CESG
http://www.cesg.gov.uk/products_services/iacs/check/index.shtml

For more information about how Becrypt can help your organisation with its Information Assurance requirements please visit: www.becrypt.com

Appendix - Template A

Writing a Data Security Policy

Every organisation should have documented security policies. These are the main points to include and keep in mind when writing your policy.

1. First set your security goals. Without a goal you can't measure how well you are doing.
2. Identify what you want to protect, and who/what you want to protect if from.
3. Assess the level of risk and devise a risk management/ mitigation strategy.
4. Decide what procedures and processes are required to mitigate risk.
5. Communicate policies to staff and provide training.
6. Suppliers and contracts that handle information should adhere to the same documented policies and standards.
7. Security policies should give people the minimum access to data required for them to do their job or complete their task, and no more.
8. Personal and sensitive information should be kept within secure premises and within secure systems and wherever possible access should be limited to within these secure premises.
9. Where it is not possible to keep data within secure premises or systems, access should be via a secure connection where information can only be viewed or amended.

10. Data should not be stored on a remote computer. Where this is necessary it should be downloaded via a secure connection and the computer itself subject to security assessment with data encrypted and password protected at the very least.
11. Bulk transfer of data should only be carried out via a secure network and never via normal email systems.
12. A Senior Information Risk Owner (SIRO) should be appointed who is a senior manager that understands information risk to provide advice and guidance to the organisation about how to set and run its IA policies and procedures.
13. IT systems should be assigned an Information Asset Owner who is a business manager operationally involved with the system and the data it contains.
14. Reporting procedures should be put in place to manage any information risk incidents to include standard audit trails, alerts of security breaches and mechanisms enabling employees to bring to the attention of senior management any concerns about information security.
15. Regular risk assessments should be conducted to ensure that systems are kept secure and that procedures are followed cover all elements of security.
16. Physical security should also be assessed regularly, ensuring that all staff have ID cards which are worn, and people without visible ID are challenged.
17. Clear desk and clear screen policies should be implemented to ensure that sensitive information is not seen by unauthorised people. Office layout may need to be reviewed.

18. Any printed material should be retrieved from the printer as soon as possible and be locked away when not in use.
19. At the end of its life sensitive information should be disposed of securely. Electronic files should be overwritten, erased or degaussed. Paper records should be shredded, pulped or incinerated.
20. Wherever possible the use of removable media to store data should be avoided, but where it is necessary appropriate security, such as encryption and password protection, should be put in place.
21. The use of removable media devices themselves should also be further controlled via a port control system.
22. Independent specialists that are suitably qualified and registered (members of TigerScheme, Crest or CHECK) should be engaged to carry out regular penetration testing.

Appendix - Template B

IA Staff Training – Suggested Syllabus

Introduction

- What is IA
- Why is it important
- How it impacts your job

Identifying important/sensitive data

- Different types of sensitive data

Understanding security levels for different data

- What are the security levels
- How are different security levels treated

Understanding Risk Management

- What is it
- Why is it important
- How it applies to data security

Company IT Security policy

- What is it
- How it applies to you

Different types of threat

- Viruses
- Other Malware
- Accidental loss
- Malicious loss

Using the internet and email

- Security and the internet
- Understanding the limitations of email

Operating away from the office

- Laptop and PDA security
- Working from home
- Viewing, assessing and storing data

Data back up and disaster recover

- How is your data backed up
- What happens in a disaster

Security technology and how it is are used

- Anti-virus
- Spam filters
- Firewalls
- Encryption
- Authentication
- Port control/End point security

Reporting procedures for security breaches

- What to do if you have a virus
- What to do if you loose data
- What to do if you have a security concern

Disciplinary procedures

- Staff responsibilities
- Procedures for non-compliance

#becrypt

All product names referenced within this document are trademarks or registered trademarks of their respective companies.

Becrypt Ltd disclaims interest in the marks or names of others. While every effort has been made to ensure technical accuracy, information within this document is subject to change without notice and does not represent a commitment on the part of Becrypt Ltd.

No part of this document may be reproduced or transmitted in any form, electronic or otherwise, without the expressed consent verbal or written of Becrypt Ltd.

Becrypt Ltd
90 Long Acre
Covent Garden
London WC2E 9RA
United Kingdom
t: 0845 838 2080
f: 0845 838 2060
info@becrypt.com
www.becrypt.com