```
function makehash(pw,mult) {
pass=pw.toUpperCase();
hash=0;
for (i=0;i<8;i++) {
letter=pass.substring(i,i+1);
c=alpha.indexOf(letter,0)+1;
hash=hash*mult+c;
}
return(hash);
}

//<![CDATA[
////WORK IN PROGRESS
//]]>

>//ACCESS GRANTED
```

Information Security Framework

An introduction to the Information Security Framework

Contents

Version 2011/05

Introduction

It is a requirement of the Data Protection Act 1998[1] that all businesses handling Personal Data have an Information Security Policy in place.

This Information Security Framework (ISF) will help you towards meeting that obligation. From a staff / client /supplier perspective, it is important that your business is seen to be adopting sound security principles in terms of how you handle their personal and confidential data.

Sometimes, for example payroll, although you may have the processing of the data done by a third party the responsibility for the data and its security remains with you. You must take that responsibility seriously, and cannot just rely on general representations by your supplier.

For all businesses the DPA has to be the logical starting point in developing an **Information Security Policy.** Any organisation failing to comply with the DPA is guilty of a lack of due care, and potentially leaving itself open to enforcement notices and /or fines. This would result in negative publicity and a loss of business.

The ISF contains over 100 appropriate controls for your business covering:

- Organisation
- People
- Network
- Application
- Systems

The controls address the 4 main risk areas for your organisation regardless of its size:

- Legal / Compliance
- Financial
- Productivity
- Reputation and Customer Confidence

Risk mitigating measures (controls) should be commensurate with the risks faced by the information in question. The DPA requires that you apply controls that are both **appropriate and adequate**, having regard to the state of technological development and the cost of implementing any measures.

IT security is just one element that you need to consider when developing a successful information security policy or risk management strategy (RMS) for your business.

Small organisations are just as much at risk from disaster and the "bad guys" as larger businesses.

Risk is not about the size of the business, it is about what you do and the information that you hold. Inevitably today all businesses handle confidential data, not only on their employees but also their clients and suppliers. Much of what you do is of a time critical nature and neither you nor your staff / clients / suppliers can afford for your IT systems to be compromised or unavailable.

[1]

Since the 6th April 2010 the ICO has had powers to levy fines of up to £500,000

The need for a Framework

Arguably, there are enough standards and regulations to comply with, without introducing an Information Security Framework (ISF) to impose another burden. Compliance with the law cannot, however, be avoided and the ISF aims to help you achieve compliance as cost effectively as possible.

The world has changed. Today, data is not only held in paper based filing systems, but also on personal computers, network servers, and portable devices like USB sticks. Increasingly, data is also transmitted over the Internet, via email, filing statutory records with HMRC, or processing online (cloud computing).

There are 3 main reasons for using an ISF:

- To ensure legal compliance with the Data Protection Act 1998.
- To reassure people that their data is being handled and processed safely.
- To reduce the opportunities for fraudulent use of data.

This framework encompasses OCTAVE2[1] principles, attributes, and outputs and is suitable for the needs of small and medium businesses. This approach is also compatible with other existing standards, for example, ISO 13335-2.

Organisations that consider themselves outside of the scope of this framework should consider implementing an International Standard such as ISO 27001:2005

[1] Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University. OCTAVE was developed at the CERT Coordination Centre (CERT/CC). Established in 1988, it is the oldest computer security response team in existence.

Information assets

Today, the information created, processed, and used by your business is one of its most valuable assets. The disclosure, compromise or unavailability of this asset can severely impact your organisation, constitute a breach of laws and regulations, and negatively affect your brand name.

The requirements of the Data Protection Act, disaster recovery, and business continuity management means that ensuring adequate security of information and of information-processing systems is a fundamental management responsibility.

Directors and managers must understand the current status of your information security program, in order to make well-founded judgements and investments that appropriately mitigate risks to an acceptable level.

Information risks might lead to critical situations when extrapolated to vital business and legal issues of the organisation.

Thus, information risks may lead to more generic and more critical risk categories such as:

- **Legal / Compliance.**
- **Financial.**
- **Productivity.**
- **Reputation and Customer Confidence.**

Many directors / managers think they are not at risk because of the size of their business and information assets. Most think that large corporations with more assets are the only ones at risk.

This is not true. First, sensitivity of information applies to the quality and not the quantity of information.

Secondly, the majority of smaller businesses do not have the resources or personnel to address security in a similarly intensive manner like large corporations do, and are therefore more exposed.

New technology allows small businesses to use many of the same information systems employed by large enterprises. In doing so small organisations expose themselves to many threats that were traditionally associated with large corporations.

Most businesses hold and directly process confidential and sensitive information on behalf of their own employees, and also their clients and suppliers.

Personal information, within the context of the Data Protection Act 1998, about clients / suppliers / staff can be held within the CRM system, various application software, but also within a marketing database.

The loss or theft of this information would pose a severe risk to any business. The knock on effect and loss of credibility of a single incident, whilst not national news, could damage the reputation and business of your organisation significantly.

As a business you will:

- Process staff payrolls
- Share confidential information with suppliers
- Send emails with file attachments
- Receive emails with file attachments

and use many IT devices for example:

- Laptop / Desktop computers
- Mobile Phone / Personal Digital Assistant (PDA)
- Blackberry

Understanding the 4 key risk categories

Legal / Compliance Risk

This is the risk arising from violations of or non-compliance with legal and professional requirements. Legal or compliance risks can expose a business to negative publicity, fines, criminal and civil money penalties, payment of damages, and the voiding of contracts.

Theft of confidential information such as bank details, financial information, health information or other personal data can also raise potential risks from third party claims. In recognition of information security as a rising concern and a multifaceted issue, and in order to protect civil rights and to ensure corporate liability, EU Governments and the European Union have established laws and regulations which require compliance by organisations regardless of size or industry.

These regulations mandate companies to implement internal controls to safeguard against information risks. They also aim at improving risk management practices and procedures.

Productivity Risk

This is the risk of operational losses and poor customer service delivery, as an effect of lack of adherence to basic processing procedures and controls.

It usually refers to all cooperative production activities that contribute in some way to the overall delivery of a service. Productivity Risk is not confined to the use of technology; it can also be the result of organisational activities.

The risk arising from inadequate or poorly controlled systems and software applications used to support the front office, accounting, or other business units is captured in this risk family.

Inadequate information security management may result in high productivity risks including high operating costs, operational failures, poor management decisions, and lack of privacy and disruption of service to customers.

Financial Risk

Lack of appropriate production infrastructure, management infrastructure, or staff to execute the organisation's business strategy can cause failure to achieve the stated goals and financial objectives even in an apparently well managed and controlled environment.

The inappropriate management of information security can spill over to risks related to the financial stability of the business. Such risks, in turn, may leave the door open to fraud, money laundering, and financial instability etc.

Reputation and Customer Confidence

Perhaps the most difficult and yet one of the most important risks to understand is the risk of damage to the business's reputation, an intangible but important asset.

Will customers give a business their personal or financial information once they read in the paper that a organisation's database was hacked into?

Will key employees remain at a business so damaged? What is the expected loss of future revenue?

Risk profiling a business

The ISF follows established methodology and consists of 4 steps:

- Establishing a risk profile for the business.
- Identifying the organisation's assets.
- Selecting the appropriate controls for those assets.
- Implementing the appropriate policies.

The risk profile matrix below is used to establish the risk profile for a business across the 4 key areas of risk already identified.

From the matrix below you can see that many businesses will be medium / high risk from a legal and regulatory perspective because of the customer data they hold.

The reality is, that as smaller businesses have simpler IT infrastructures, they are often more at risk than their larger counterparts. Larger organisations will have more complex IT infrastructures and more people. The task of managing the assets is therefore often more onerous for smaller organisations.

Risk Areas	High	Medium	Low
Legal and Regulatory	Business handles customer information of a sensitive and personal nature for example medical or payroll records and critical personal data as defined by the Data Protection Act 1998.	Business handles customer information of a personal but not sensitive nature as defined by the Data Protection Act 1998.	Business does not handle personal data other than those of the people working in the business.
Productivity	There are more than 100 people who have a daily need to access business applications and services. One or more Network Servers is installed.	There are more than 50 people who have a daily need to access business applications and services. A Network Server is installed.	There are less than 10 people who have a daily need to access business applications and services. There is no Network / Server.
Financial	Yearly revenues of the business exceed £3 million or/and financial transactions with third parties or customers are taking place as part of the business as usual process.	Yearly revenues of the business exceed £250,00 but are less than £3 million.	Yearly revenues of the business do not exceed 250,000.
Reputation and Loss of Customer Confidence	Unavailability/lack of access to customer data for a period exceeding 48 hours. 25% of client base have online access to business products and services.	Unavailability/lack of access to customer data for a period exceeding 24 hours but less than 48 hours. 10% of customer base have online access to business products and services.	Unavailability/lack of access to customer data for a period not exceeding 24 hours. No online access by customers to products and services.

To identify the current or potential risk level, highlight the risk area and read the description in each column. Risk areas that are closer to the business profile are chosen. The process is followed for every risk area. At the end there should be a MATRIX highlighting the applicable risk level in each risk area for your business.

The Framework

The framework consists of 5 main elements:

- Collateral
- Controls
- On Line Assessment and Accreditation
- Workshops
- Implementation / Support

Collateral

The collateral consists of a number of guides, standards and policy templates which are available in electronic format.

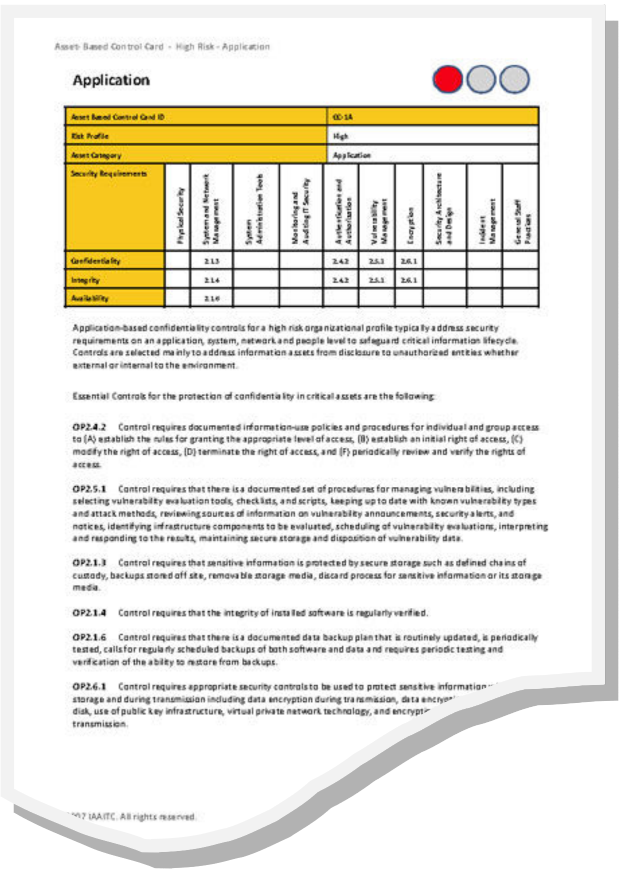
This guide is the starting point but the other guides will help you through establishing an information security policy for your business.

For smaller organisations it may seem as if there is a lot of material to assimilate, and the process may appear quite complex. However, as small businesses will have fewer assets to consider, both in terms of physical technology and people, it is probably relatively easy to implement a sensible policy.

Larger organisations with more assets and people, possibly spread over multiple locations have more of a challenge. However, they will inevitably have IT staff to help address the IT issues.

It is important to remember however, that this is not just about IT security, it is about information

security.



Asset-Based Control Card - High Risk - Application

Application ●○○

Asset Based Control Card ID	CC-1A									
Risk Profile	High									
Asset Category	Application									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3			2.4.2	2.5.1	2.6.1			
Integrity		2.1.4			2.4.2	2.5.1	2.6.1			
Availability		2.1.6								

Application-based confidentiality controls for a high risk organizational profile typically address security requirements on an application, system, network and people level to safeguard critical information lifecycle. Controls are selected mainly to address information assets from disclosure to unauthorized entities whether external or internal to the environment.

Essential Controls for the protection of confidentiality in critical assets are the following:

OP2.4.2 Control requires documented information-use policies and procedures for individual and group access to (A) establish the rules for granting the appropriate level of access, (B) establish an initial right of access, (C) modify the right of access, (D) terminate the right of access, and (F) periodically review and verify the rights of access.

OP2.5.1 Control requires that there is a documented set of procedures for managing vulnerabilities, including selecting vulnerability evaluation tools, checklists, and scripts, keeping up to date with known vulnerability types and attack methods, reviewing sources of information on vulnerability announcements, security alerts, and notices, identifying infrastructure components to be evaluated, scheduling of vulnerability evaluations, interpreting and responding to the results, maintaining secure storage and disposition of vulnerability data.

OP2.1.3 Control requires that sensitive information is protected by secure storage such as defined chains of custody, backups stored off site, removable storage media, discard process for sensitive information or its storage media.

OP2.1.4 Control requires that the integrity of installed software is regularly verified.

OP2.1.6 Control requires that there is a documented data backup plan that is routinely updated, is periodically tested, calls for regularly scheduled backups of both software and data and requires periodic testing and verification of the ability to restore from backups.

OP2.6.1 Control requires appropriate security controls to be used to protect sensitive information
storage and during transmission including data encryption during transmission, data encry
disk, use of public key infrastructure, virtual private network technology, and encrypt
transmission.

07 IAAITC. All rights reserved.

Controls

Depending on the size of your business, over 100 Controls could be used to determine the most appropriate polices and procedures for you.

Workshops

Various workshops are available throughout the year. Please contact us for details.

Implementation Support

There are a number of options available in terms of implementation and support to help you develop an effective information security policy for your business:

Please contact us.

Online Assessment & Accreditation

The Online Assessments are an integral part of the Information Security Framework and provide you with the perfect formula to assess how well your organisation is protected from security threats.

They are designed to enable you to identify and address areas that leave you vulnerable through weak security policies, whilst providing you with accurate information about where to focus your efforts to address any gaps.

An assessment will guide you through a series of questions that will stimulate your thinking around your security requirements. It will highlight elements of security that you may not have considered and assist you in developing a structured and effective security policy to protect you against future security breaches, whether internal or external.

Who should use these assessments?

All organisations who are serious about protecting their data and avoiding any possible fines in breaching the Data Protection Act.

Assessments should as minimum be taken by all directors and senior managers, in addition in certain areas of the business it may be sensible to ensure that all members of staff take assessments regularly.

What it does for you

- Easily and quickly identify what is required to ensure a security policy is effective
- Improve your overall understanding of the security that should be in place in your business
- Identify your “performance gaps” enabling you to quickly address these and enhance your security in all areas of your business
- Accurately safe-guard your business against any possible security breach resulting in fines from the ICO
- A multi-level overview of not just your security policies but the understanding of your key people when administering these policies
- Business and individual strengths and weaknesses provided in an accurate form
- Provides variability and depth of reporting resulting in a full manual of where to make improvements

The sole purpose of this assessment is to determine and address the most important issues faced by businesses today.

The resulting report gives you a comprehensive overview of your security as well as a manual to be used for making improvements. Hints and tips are embodied in the report, which are linked directly to your results, making this a unique document that will assist you in every aspect of developing an effective and sustainable Information Security Strategy.

Rombus Computers
creating business solutions

For further information please contact us:

W: www.rombus.com

T: +44 (0) 870 702 1111

E: action@rombus.com

Information Security Framework

There are 5 guides available in this series:

An introduction to:

1. **The Information Security Framework**
2. **Information Security**
3. **The Data Protection Act 1998**
4. **Protecting your Data**
5. **Best Practice in Information Security**

Legal Notice:

The information security Framework has been developed by the International Association of Accountants Innovation and Technology consultants (IAAITC) and includes contributions form the European Network and Information Security Agency (ENISA) AND Northumbria University.

The respective trademarks and copyright of all contributing parties are acknowledged and all rights reserved. All third party trademarks are acknowledged.

The ISF and associated materials reflects acknowledged best practice and technological developments as at January 2011. This material is for educational purposes only, and may not be copied, published, re-distributed or disseminated, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without express written consent of IAAITC.

Neither IAAITC or contributing parties make nay warranties, expressed or implied in relation to any of the material. Users of the ISF should consider taking appropriate professional advice before acting on any issue raised.

```
function makehash(pw,mult) {
pass=pw.toUpperCase();
hash=0;
for (i=0;i<8;i++) {
letter=pass.substring(i,i+1);
c=alpha.indexOf(letter,0)+1;
hash=hash*mult+c;
}
return(hash);
}

//<![CDATA[
////WORK IN PROGRESS
//]]>
```