Resources for Chapter 2 – Information security governance

RESOURCES

- **Template for an information security policy**
- **Responsibilities overview: Information ownership and risk management – Cardiff University**
- **Developing an information security policy – University of York, case study**
- **Bringing information security strategy to senior management – UCL, case study**
- **Key questions for top management**
- **Example of a presentation to sell the concept of an ISMS to top management**

Template for an information security policy

<ORGANISATION>: Information security policy

Introduction

[ORGANISATION]'s computer and information systems underpin all [ORGANISATION]'s activities, and are essential to [ENTER MAIN BUSINESS/FUNCTIONAL OBJECTIVES HERE].

The [ORGANISATION] recognises the need for its members, employees and visitors to have access to the information they require in order to carry out their work and recognises the role of information security in enabling this.

Security of information must therefore be an integral part of the [ORGANISATION]'s management structure in order to maintain continuity of its business, legal compliance and adhere to the University's own regulations and policies.

Purpose

This information security policy defines the framework within which information security will be managed across the [ORGANISATION] and demonstrates management direction and support for information security throughout the [ORGANISATION]. This policy is the primary policy under which all other technical and security related policies reside. [ENTER ANNEX LINK HERE] provides a list of all other policies and procedures that support this policy.

Scope

This policy is applicable to and will be communicated to [EXAMPLE: all staff, students and other relevant parties including senior and junior members, employees, visitors and contractors].

It covers, but is not limited to, any systems or data attached to the [ORGANISATION]'s computer or telephone networks, any systems supplied by the [ORGANISATION], any communications sent to or from the [ORGANISATION] and any data - which is owned either by the University or the [ORGANISATION]- held on systems external to the [ORGANISATION]'s network.

Organisation of information security

The [HEAD OF DEPARTMENT] is ultimately responsible for the maintenance of this policy and for compliance within the [ORGANISATION]. This policy has been approved by [SENIOR MANAGEMENT GROUP] and forms part of its policies and procedures.

[SENIOR MANAGEMENT GROUP] are responsible for reviewing this policy on an annual basis. They will provide clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.

The [INFORMATION SECURITY ROLE] is responsible for the management of information security and, specifically, to provide advice and guidance on the implementation of this policy.

[OPTIONAL DEPENDING ON ORGANISATION SIZE]

The [INFORMATION SECURITY ADVISORY GROUP] comprising representatives from all relevant sections of the [DEPARTMENT/COLLEGE/OTHER UNIT] is responsible for identifying and assessing security requirements and risks.

It is the responsibility of all line managers to implement this policy within their area of responsibility and to ensure that all staff for which they are responsible are 1) made fully aware of the policy; and 2) given appropriate support and resources to comply.

It is the responsibility of each member of staff to adhere to this policy.

Policy Statement

The [ORGANISATION] is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training and awareness for information security and to ensuring the continued business of the [DEPARTMENT/COLLEGE/HALL]. It is the [ORGANISATION]'s policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance.

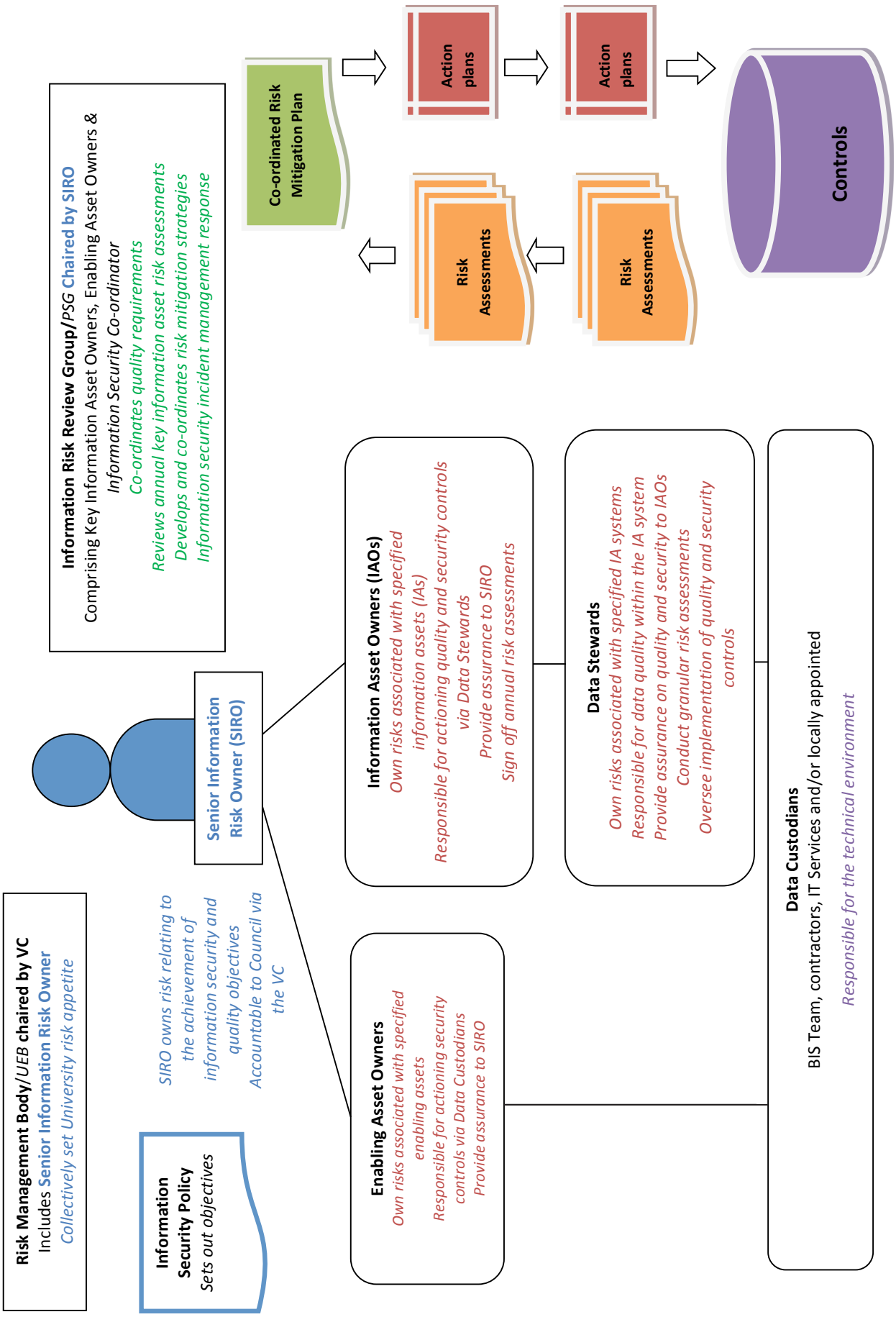
To determine the appropriate level of security control that should be applied to information systems, a process of risk assessment shall be carried out in order to define security requirements and identify the probability and impact of security breaches.

Specialist advice on information security shall be made available throughout the [DEPARTMENT/COLLEGE/OTHER UNIT] and advice can be sought via the University's Information Security Team [ADD URL] and/or [ADD ADDITIONAL URLS, if required].

It is the [UNIT NAME]'s policy to report all information or IT security incidents, or other suspected breaches of this policy. The [UNIT NAME] will follow the University's advice for the escalation and reporting of security incidents and data breaches that involve personal data will subsequently be reported to the University's Data Protection Officer. Records of the number of security breaches and their type should be kept and reported on a regular basis to the [SENIOR MANAGEMENT GROUP/INFORMATION SECURITY ROLE].

Failure to comply with this policy that occurs as a result deliberate, malicious or negligent behaviour, may result in disciplinary action.

Responsibilities overview: Information ownership and risk management – Cardiff University



Developing an information security policy – University of York, case study

Like many organisations, in York we knew that our existing regulations and policies were old and increasingly inadequate. Research contracts were asking for policies which aligned with ISO/IEC 27001, our auditors were commenting on lack of policies, and IS/IT staff wanted more policy, both general and detailed to solve problems.

We had existing policy on Data Protection, Freedom of Information, Records Management and IT operations. This gave us a way of establishing the hierarchy of the new policies- but all the existing policies were rewritten during the course of the work.

Our first attempt was to take the specimen policies in the previous UCISA Toolkit and set about editing them. We thought this would be quick, but it turned out to be a disaster. The policies were too general, and in many cases did not fit with our institutional ethos. We found that such key policies are very institution based - specimen policies help to guide but very the real policies are very much about what will be tolerated and work in the setting of a given institution.

For our second attempt, we started from scratch. We agreed with institutional senior management an approval process for Information Security policies and drafted a list of policies that we needed based on ISO/IEC 27001. In our first attempt, we used existing committee structures to approve policy and the delays introduced were very large. For the new process, a senior member of staff was delegated power to approve policies in this area, with only policies that were felt to be contentious or that affected other areas taken to committee.

From there, we defined the general format of a policy. For us, a policy was to be a short (two page max) document at a high level. Underneath each policy there would be method statements and guidance containing the detail. We also agreed some basic definitions and use of terminology (e.g. *must vs. should*).

Next we agreed some overall principles:

- our aim was to help people to use data safely, not lock it away and make it hard for people
- the policies should apply to all data, irrespective of format (paper or electronic)
- avoid jargon
- exploit current good practice, introducing changes only where necessary
- we would not do any publicity or training until most of the policy suite was in place

These framework and principles helped us to get past some initial stumbling blocks around format and ensured that the suite of policies have a consistent feel, with common section and definitions and gave us some high level principles to help clarify what was in scope and not in scope for the policy suite.

Finally we agreed to avoid wide consultation early on in the process. We found it better to have something which has been worked on and is in quite good shape before opening it up for wider consultation. Without a specific document to focus on, we found that people found the issues hard to grasp and discussions were very unfocussed.

Once we had that overall process agreed, we started working our way through the list. We found some tricky issues during the process and, as ever, progress was slower than we expected in advance but overall, we have made good progress.

Even after a year of work, we are not done. Some of the subsidiary policies are not done and we are only just starting awareness raising but the policies are being referenced when new projects are started or bids submitted, the auditors are happier and external funders are being assured that the University can handle sensitive research data in a secure fashion.

Summary

- Create policies tailored to your environment; do not copy templates blindly
- Provide well-developed documents for wider consultation, rather than a very initial draft
- Develop and agree a simple approvals process

Bringing information security strategy to senior management – UCL, case study

At UCL, we began to formalise our information security strategy in late 2012, when the post of Head of Information Security was created.

The first stage involved finding out what was already happening, not on the process/controls level, but on the strategic and governance levels. We discovered the following:

- An existing UCL-wide risk management process, which was under further development
- The IT department was working to implement ITIL for improved process management and better customer service.
- There was a major University initiative to formalise project management.
- A role handling data protection and Freedom of Information, in the Legal Department
- A PCI DSS governance role in the Finance Department
- A Records Manager in the Library with responsibility for setting data retention policy
- A project underway to provide a secure data storage and processing facility (the Data Safe Haven project) in the School of Life and Medical Sciences. This project had already requested participation from the Information Security area.

All of the above activities revealed both organisational structures and roles with which information security management activities would have to interoperate, and existing processes which we could use or adapt.

But, although we could already see how to link information security management to some existing processes (e.g. risk management), and could see some new processes we'd need, we could not actually make any changes until we had top level buy-in: and a strategy.

We started by establishing how changes to top level university activities were normally raised, discussed and approved. It turned out that the existing management hierarchy was clearly defined and provided us with a route which looked as if it could work: through the Security Working Group and a number of other committees to the Senior Management Team of the University.

In parallel to my identification of a suitable and effective way to get the material to senior management, we began to write up an actual strategy.

Initially, we chose to create a presentation in order to keep the structure as fluid as possible, and to provide flexibility in presenting it- we could vary the path through the presentation dynamically to adapt to the audience. This also had the added benefit that we could easily present it in person for feedback during its development, rather than mailing out a document. This gave us immediate and frank feedback (e.g. if people fell asleep!) as well as the opportunity to get lots of practice in explaining the material to each audience.

While it was being developed, the presentation/strategy was presented to people and groups going up the management chain to senior management, so that each group could have a say in the content and it could continue to evolve. The net effect was that it would not, by the time it reached senior management, be a single person's take on what needed to happen, but a consensus and (hopefully) already acceptable approach. At each level, we asked for permission (and sometimes was urged) to take it to the next step in the governance chain.

The golden rule we adhered to during the development and presentation of the strategy was that, at the time of the presentation of the strategy to senior management, there should be no surprises on either side. A strategy without a suitable foundation would be less likely to be accepted. On the downside, the "excitement" was inevitably going to be diminished- but in information security and management, excitement is not generally conducive to effective operations...

To make the suggestions in the strategy more likely to be well received in a meeting with senior management, we realised that we should not rely on one route alone. It also seemed sensible to try out the draft strategy on individual members of the senior management team, to get feedback and suggestions. One obvious venue was the governance body which had arisen within the School of Life and Medical Sciences to manage sensitive data. We presented the draft strategy at one of the meetings, and received a huge amount of helpful suggestions. The ones which made the most impact were:

- It should be shorter (at the time, it ran to 60 slides...).
- It should relate to existing top level priorities. We had an overall University Strategy and five year plan- this strategy should relate directly to them.
- It should contain concrete examples- e.g. how much money could be saved by avoiding incidents.
- It should not require explanations- it should make sense by itself.

Following this meeting, the strategy was revised and improved significantly, and began to look like something which senior management would be happier with. we did not, however, add content to promise specific cost savings, as it would not have been based upon reliable data. One thing we did add to improve the immediacy of the proposal was a short list of recent incidents affecting universities.

With the strong support of my line management, and after about ten months of preparation, we were authorised to present the proposed strategy to senior management. Since the meeting format did not permit the use of presentations, we summarised the

strategy into two pages of A4 text. This was a critically important step, as it stripped the strategy and its justification back to essentials, and vastly improved them as a result.

When the date of the meeting arrived, the topic was scheduled for 10 minutes total - five minutes on the standard information security update, and five minutes on the strategy.

At the meeting, the group took some considerable interest in the information security update, but showed even greater enthusiasm for the strategy, which received unanimous support. In the end, the information security section of the meeting stretched to over 20 minutes.

The substantive feedback from UCL's senior management team was as follows:

1. They agreed to support the proposed strategy as presented.
2. They approved initial organisational changes to embed information risk management into normal operations, including the introduction of senior information risk owners at Faculty level.
3. They recognised that culture change was important to the success of information risk management across UCL.
4. They were strongly in favour of an awareness programme to improve attitudes to information risk.

Now the real work begins. We have an approved strategy, but need to make it happen. The challenges at hand are really high level and pervasive, such as culture change, and technical capabilities. The next steps we are going to take are the formalisation of information risk management across UCL, the implementation of an awareness programme, and further engagement with departments and faculties to understand their ways of working, risks and needs.

Summary points

- Ensure you know how risk management is already working.
- Find out the accepted route for new ideas to be received, assessed and approved, and use it.
- Be patient: big changes which are going to stick take time to get going.
- Ensure that the strategy evolves as you present it to more people, so that it is fit for purpose.

Key questions for top management

The university environment has some characteristics which influence the way in which information security can be managed. The organisation's senior management team, or "top management", having overall responsibility for information security, must consider these characteristics when designing the ISMS.

Federation

Not all the information technology used within an organisation is provided (or indeed controlled) by a central IT service. This is particularly the case with IT supporting research but may also be the case in collegiate institutions or those that have a high degree of devolution. Similarly there may be specific administrative functions within departments or colleges. However, the impact of any information security breach is likely to be on the organisation, not the department.

- How do you ensure buy-in from those departments/units that operate semi-independently?
- Who, in those departments, is responsible for information security and how do they link with the institutional information security operation?
- How do you ensure that IT systems that are not under central control meet a base level of security (such as the Cyber Essentials promoted by BIS[1])?

Suggestions:

- The Senior Information Risk Owner (see Chapter 8, Roles and competencies), as part of their role, should take responsibility for selling information security to devolved departments.
- It may be appropriate for there to be a Senior Information Risk Owner for each devolved operational unit. These would have responsibility for championing information security policy and requirements within their department.
- A hybrid approach to technical security may be adopted where a base level of security is required for a given classification of information, but each operational area is provided with the tools to implement controls as they see fit. Relies heavily on independent support and oversight, quite time consuming as there is no economy of scale for a number of things.

Autonomy

Academic staff involved in research often operate with a degree of autonomy. They bid for funding and are responsible for the use of those funds to deliver the specified research. The requirements of that research may result in the development of bespoke IT systems. Although these are effectively production systems, they are largely unsupported and may present an information security risk. Staff can and do go to retail outlets and purchase IT equipment for use in the organisation, particularly for research. Such equipment may not meet the standards of the organisation.

- How do you ensure researchers understand the sensitivity of the information they collect and store?
- Does your research ethics policy take into account information security issues?
- Do you know where collections of personal or sensitive data used in research exist?
- Do you have a procurement policy that restricts the purchase of equipment to a defined and supported product set?
- Do you have a storage strategy that mitigates the need for researchers to purchase storage outside of the institutional purchasing procedures?

Suggestions:

- Researchers that are working in departments where they are likely to utilise personal or sensitive information should be regularly given awareness training and refresher courses;
- As a minimum, the minutes of research ethics committees should be forwarded to the information security group to allow them to advise on appropriate security measures, and log the existence of sensitive data collections.
- Consideration should be given to mandating procurement of IT equipment through established procedures to ensure that all equipment is to a standard that may be supported by the IT function.

Home working and use of personal devices

Use of personal devices such as phones, tablets, etc by both staff and students for handling organisational information has increased to almost become the norm. Students look to access resources remotely in order to write and submit coursework, to revise, etc.

[1] https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

Organisations increasingly accommodate home working for their staff as part of flexible working practices. Visitors bring their own devices onto the campus and access resources either within the organisation or from their own organisation. Each form of access presents a risk to information security.

How are the security risks associated with personal devices accommodated in your policies and procedures?

Suggestions:

- The location of the key information assets in your organisation needs to be known and understood and appropriate measures taken to protect them.
- It may be appropriate to restrict home working to trusted devices provided by the organisation and with appropriate security measures already in place.
- The wireless network may be deemed to be untrusted given that personal devices may connect to it with little or no verification. Consequently the organisation may consider placing a firewall between the wireless part of the network and the main campus network.

Unclear boundaries

The individuals who access an organisation's information are not just restricted to traditional definitions of staff and students. The permanent staff may be supplemented with visiting lecturers, research collaborations will require staff from other universities to have access to resources, alumni may have access to resources, employees from other organisations may take part in professional development activities, etc. The physical boundaries of an organisation may not be restricted to the organisation alone as buildings can be shared with commercial entities which are spun-off from research projects, and which use the same facilities as the organisation itself.

In some cases, access to resources is provided to individuals that are never physically present. The increase of distance learning means that the organisation may virtually extend to all corners of the globe. Some universities have sought to extend their reach by engaging in partnerships with overseas institutions or by setting up overseas campuses.

- How are the information security requirements of the organisation communicated to non-traditional members of the organisation?
- Should any special measures be applied to off campus students or staff?
- Were information security policies considered when the decision was made to establish an overseas campus?

Suggestions:

- There needs to be a readily accessible way of making such members of the organisation aware of information security and their responsibilities for ensuring that the organisation's policies are adhered to.
- The organisation may need to consider adherence to information security policy as part of any tenancy arrangement for external organisations.
- Access to resources and systems should be time limited for temporary staff.
- There should be processes in place to determine the appropriate levels of access to organisational resources and systems for all members of the organisation.
- Organisations should consider the legislative requirements of nations where overseas campuses are being established and their impact on the institutional information security policy as part of the planning process.

Openness, sharing and cyber security initiatives

There is a drive towards making the outputs from research and the data behind it publicly available. Researchers, on the other hand, have built their reputations on the research they have produced and are looking to protect their intellectual property. In addition, the Government is also pressing the higher education sector to take appropriate steps to protect the intellectual property that is generated within the organisation. The organisation will need to balance openness with the requirements to protect key research and information assets.

- Are the requirements of open access well understood at your institution?
- Have the resources been committed to meet the requirements for the sharing and archiving of research data?
- Are the locations of research data that may result in commercial benefit to the organisation known?
- Suggestions:
- The balance between openness and individual academics' desire to protect their intellectual property is a political, not information security, issue. The organisation's top level management should drive the policy for open access.
- Research that may deliver a commercial benefit to the organisation should be treated as a critical information asset and protected as such.

Commercial relationships

Some research is conducted in association with or on behalf of commercial organisations. Consequently there may be specific security conditions included in the research contract to ensure that the data are protected.

- Does your organisation take a lead in defining the security requirements for commercially sensitive research data?

Suggestions:

- A structured approach should be in place to manage contracts which may be commercially sensitive. These should build on existing business processes and ensure legal due diligence.
- The processes should be in place to ensure that, if required, the ability to provide information security oversight can be easily demonstrated.

Communities of users

Difference categories of users will have different views on information security, different appetites for risk, and different levels of understanding of the requirements of the organisation's information security policy. Culture varies across the organisation. This is not restricted to differences between staff and students nor is it to differences between administrative and academic staff. All need an understanding of information security risks and their roles in delivering the information security policy.

- How do you accommodate a wide range of skills and experience levels when implementing an institution wide policy?

Suggestions:

- Risk management should be built into normal working practices so that staff recognise all risks, report them and take mitigating action where appropriate.
- The awareness activity needs to take cognisance of the variety of expertise, approaches and understanding members of the organisation have

Turnover

Universities are dynamic organisations with a high turnover of personnel. Some of this turnover is known and managed; student course dates are known and established processes are in place to manage registration and, on completion, graduation. However, not everyone completes their course and there need to be processes to manage exit of those students who drop out or otherwise do not complete their studies. There will be processes to manage *regular* staff entry and exit and these will usually be the responsibility of a Human Resources function, whether centralised or devolved. The processes around *ad hoc* members of staff and other members of the organisation that have access to resources and systems also need to be well managed; these processes may be devolved to a wide range of departments or functions and so may not be so well defined.

- How well is information security awareness built into your induction processes for staff and students?
- Are ad hoc members of the organisation included in awareness activity?

Suggestions:

- Tailor the awareness campaigns for each part of the organisation's community which matches the level of risk and the rate of turn over.
- There should be appropriate processes in place for induction, ongoing awareness and exit for all members of the organisation.

Example of a presentation to sell the concept of an ISMS to top management

Slide 1

Information Security Framework Programme

Slide 2

What is information security?

Protection from threats to ensure the continued:

- confidentiality
- integrity
- availability

of our information

Take definition from International Standard on Information Security Management - the ISO/IEC 27000 suite

- **Confidentiality** - ensuring that information is accessible only to those authorised to have access
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods by protecting against unauthorised modification
- **Availability** - ensuring that authorised users have access to information and associated assets when required
- **ISO/IEC 27001** sets out structure and process for implementation of an ISMS
- **Not just about IT** – physical and human aspects!!

Slide 3

What threats?

- Damage to operations
- Damage to reputation
- Legal damage

Any time anywhere and bring your own devices = multiple threats

Accidental or malicious loss of data and lack or failure of back up

Theft of personal data or IP

Inappropriate disclosure of information – breach of confidence

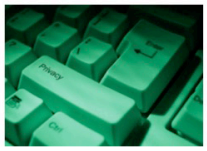
Loss of access to electronic data (viruses, denial of service)

Fines & undertakings from Information Commissioner

Inability to compete for research grants

Slide 4

The Programme's Vision



The University will operate in a manner where security of information is balanced with appropriate accessibility of that information....

...providing the optimum level of risk management to support the University's strategic goal of being a world leading institution.

It's all about risk assessment and balance – need for University approach both risk assessment and mitigation resource

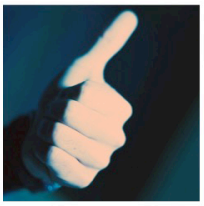
Slide 5

Where are we now?

	RAG definition
	Information Security Management System based on international standards in place. Audit trails and evidence of compliance readily available.
	Information security policies developed, risk ownership accepted and awareness improving. Comprehensive training plan agreed. Risks assessed and toolkits developed. Baseline for metrics established.
	Patchy awareness of information security. Individuals manage security within a loose policy framework. Information security risk decisions taken in isolation. No senior risk owners for information security.

Slide 6

What does the future state look like?
- *Leadership*



- Senior ownership of information security risk
- Strategic decisions about tolerable levels of risk

Importance of the risk appetite being set at a senior executive level. Looking at risk register and how we assess and accept risk. The all important strategic balance.

Slide 7

What does the future state look like?
- *Organisation*

- Information assets identified, owned and risk assessed
- Co-ordination of information security resources

ISO/IEC 27001 structured approach to implementation

Information assets – concept of ownership across the institution, e.g. 'student data' no matter where it's held

Slide 8

What does the future state look like?
- *Business Change*

- Consistent policies, procedures and decisions
- Universal tools and training
- Clear lines of accountability
- Evidence and audit

Delivering business change all important – not just an exercise in producing policies but in effecting a change in behaviour.

Slide 9

Benefits and Opportunities

Your data is safe with us!