OXFORD
BROOKES
UNIVERSITY

Project cover sheet - FOR OBIS PMO USE ONLY

Date submitted	29 July 2016	**Project ID Number**	
Project Title	Information Security Compliance - ISO27001		
Business Project Manager	Gareth Packham		
Project Executive/Sponsor	Seamus Shaw		
IT Project Manager	TBC		
Purpose	The implementation of an ISO27001:2013 compliant information security management system (ISMS) across all faculties and departments of the University, with an aim of achieving independent certification by 2019.		
Scope	TBC, All University sites, faculties and departments are expected to be within the project scope.		
Description	Achieving independent certification will require: ● A Documented risk treatment plan. ● Corrective and Preventative action procedures and logs. ● Records of technical controls with associated procedures and assessment of compliance. ● An Information classification system. ● An Internal ISMS audit procedure and schedule log. ● An Information security incident management procedure and log. ● Information security awareness training programmes. ● Independent certification from an accredited assessor.		
Strategic Importance	The less mature an information security framework is, the greater its risk of suffering a serious information security incident. The Project Aligns with: OBIS Strategy 2020: Strategic - Information Security Roadmap - Implementation for 2019		
Benefits	● Reduced risk to information assets. ● Cost savings on OBIS projects from the standardisation of information security controls and from allowing OBU to concentrate its effort and resources on specific additional security controls. ● Increased 'Brand Value' of OBU from improved security integrity. ● Independent assurance of OBU's information security management capabilities. ● An established mechanism for measuring information security performance.		

Impact of not delivering project	● An Inability to comprehensively record Brookes' information asset threats and vulnerabilities and no underlying management system to address them. ● No strategic framework for information security management across the University. ● No Feedback or knowledge of information control effectiveness. ● Poor visibility of information assets, their classification and their owners. ● Poorly documented information security policies and procedures.		
Dependencies			
OBIS work required	TBC Will Include: Adoption and application of ISO27001:2013 standards. Stakeholder Training and Education (OBU staff, Contractors, pseudo-employees, OBU Students).		
Critical resources required	OBIS Identity Management Team OBIS Senior Management Team		
Total budget required	Not Known - Verbal Update		
Proposed/required start date	September 2016		
Proposed completion date	January 2019		
PMO additional notes	We are looking to pass this through Gateway 0 and proceed to looking at delivery options and finalise the Business Case		
ITPPG recommendation	**Yes**	🟥	🟧
Date and reasons for recommendation	Recommended for approval through gateway 0, subject to policy approval and strategic buy in from the IT Programme Steering Board and Executive Board.		
ITPSB decision	**Yes**	**No**	**Defer**
Date and reason for decision / feedback to business			

IT Programme Steering Board Chair sign off ________________________________Date ___________

Project Brief

Reference number:	[Insert Project Reference Number]
Project Title:	Information Security Compliance - ISO27001
Date:	29 July 2016
Programme:	IT Master Plan
Sponsor:	Seamus Shaw (TBC)
Project Manager:	Gareth Packham
Version No:	2.0

Approvals:

1. Programme Manager
2. Project Sponsor

Distribution:

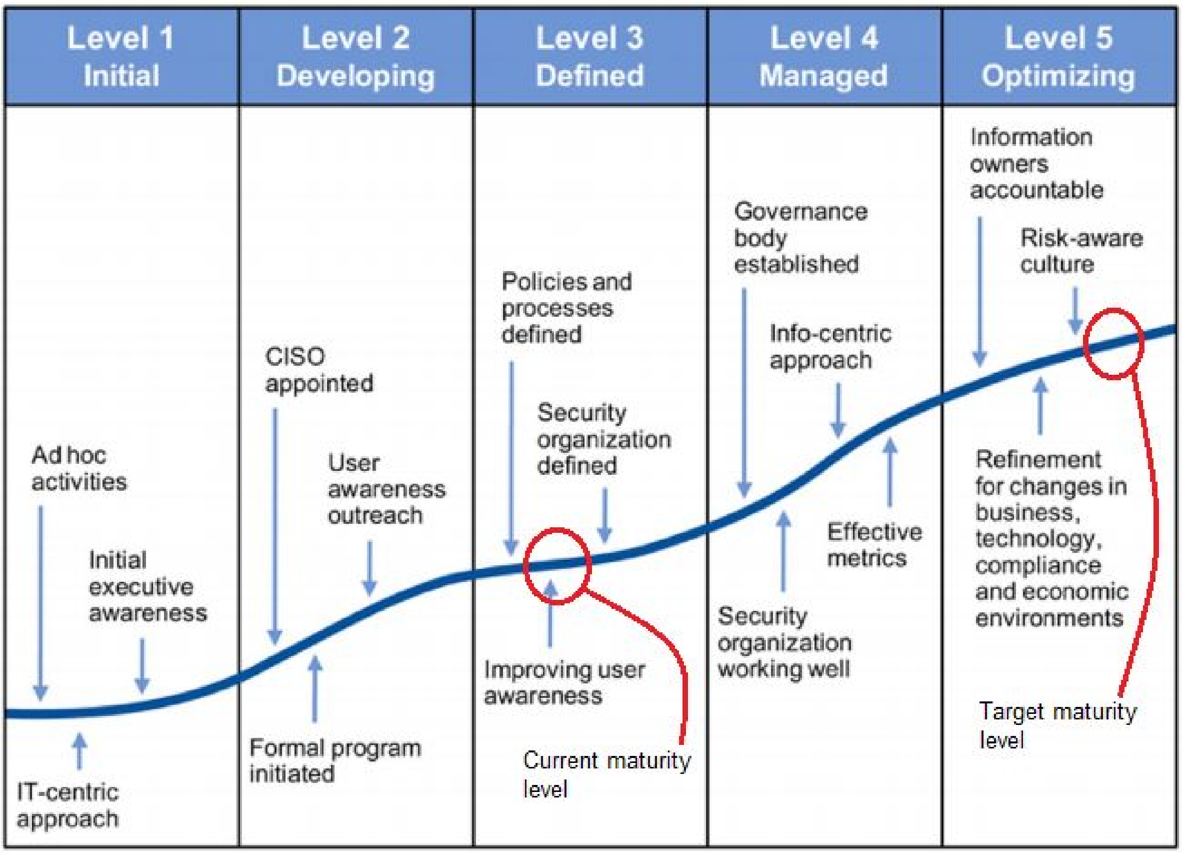
1. Programme Manager
2. Project Sponsor
3. Key Stakeholders

Project Brief

1 Background

Oxford Brookes University recognises that information and the associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals. Through its security policies, procedures and structures, the University aims to facilitate the secure and uninterrupted flow of information, both within the University and in external communications.

Although Oxford Brookes has made great strides towards effective information security management in the last few years we still lack a coherent framework with limited strategic oversight. Using the Gartner information security maturity model as a guide (see below) we can see that there is still much to do before we can consider ourselves as achieving optimal information security management practice.



Source: Gartner (June 2013)

The less mature our information security framework, the greater risk there is of suffering a serious information security incident. There have been a number of high profile data breaches at UK Higher Education institutions in the past two years, including the University of Greenwich and Queen Mary University of London. As well as media attention and subsequent damage to our reputation, information security incidents can also bring severe financial penalties. The ICO (Information Commissioner's Office) can currently fine organisations up to £500,000 for breaches of the UK Data Protection Act; if the UK chooses to adopt the new EU General Data Protection Regulations in 2018 this will increase to 4% of turnover (currently £7.2 million for OBU).

ISO 27001 (current version - 27001:2013) is an industry-standard specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

Current Information Security Risks:

a) There is currently no comprehensive record of threats and vulnerabilities to Brookes information assets with no underlying management system to address them
b) Lack of strategic framework for information security management across the University
c) No knowledge of how effective current information controls are
d) Poor visibility of information assets, their classification and their owners
e) Poorly documented information security policies and procedures

Current Information Security Issues:

a) Unable to enhanced enforce security controls for third-party suppliers / contracts

Aligns with:

- OBIS Strategy 2020[1]:
  - Strategic - Information Security Roadmap - Implementation for 2019

2 Project Definition

The overall aim of this project is to design and implement an ISO27001:2013 compliant information security management system (ISMS) across the University and achieve independent certification by 2019.

2.1 Project Objectives

a) Obtain senior management support for ISO 27001 compliance and associated information security best practices
b) Define scope of ISMS and identify interested parties, interfaces and dependencies
c) Identify all in scope information assets across the university and their associated owners.
d) Conduct business impact analysis on all identified assets
e) Develop a consistent information security risk assessment methodology and conduct a detailed risk assessment on all identified assets
f) Prepare a risk treatment plan
g) Development of an information classification and handling policy and associated guidelines
h) Carry out actions as defined by the risk treatment plan [the ISMS implementation programme]
i) Develop an internal ISMS audit function and carry out internal audits across University
j) Appoint an independent certification body and organise audit / certification visits

2.2 Project Scope and Exclusions

Determining the scope of the ISMS is part of the project itself. It is expected that all University sites, faculties and departments will be in scope.

Brookes Union is excluded from the scope of this project

[1] http://www.brookes.ac.uk/obis/it-strategy/supporting-roadmaps/

2.3 Project Deliverables

a) ISMS Scope and Framework Policy document
b) Documented information asset inventory / business impact assessment
c) Documented information security risk assessment
d) Documented risk treatment plan
e) Documented statement of applicability
f) ISMS implementation programme plan and associated documentation
g) Corrective and Preventative action procedure and log
h) Information classification system and associated guidelines
i) Record of technical controls with associated procedures and assessment of compliance
j) Internal ISMS audit procedure, schedule and log
k) ISMS metrics policy and log
l) Information security incident management procedure and log
m) Other necessary information security policies, procedures and guidelines, ensuring that these are followed
    i) Information Security Policy (existing but may not be ISO27001 compliant)
    ii) Acceptable Use Policy
    iii) Access Control Policy
    iv) Access Rights Review Procedure
    v) Change Management Process
    vi) Confidentiality Policy (existing but may not be ISO27001 compliant)
    vii) Cryptographic Control Policy
    viii) Data Protection Policy (existing but may not be ISO27001 compliant)
    ix) Data Quality & Governance Policy
    x) ICT Asset Management Procedure
    xi) Information Security Risk Assessment Procedure
    xii) Information Security Assurance / Network Security Policy (existing but may not be ISO27001 compliant)
    xiii) Information Sharing and Transfer Policy
    xiv) ISMS Internal Audit Procedure
    xv) ISMS Legal Register
    xvi) Mobile and Remote Computing Policy (existing but may not be ISO27001 compliant)
    xvii) Password Policy
    xviii) Record Management Policy (existing but may not be ISO27001 compliant)
    xix) Third party and Supply Chain Management Policy
n) Information security awareness training programme with evidence of competence
o) Pre-certification assessment
p) Independent certification from an accredited assessor.

2.4 Project Outcomes

a) Reduced risk to information assets by strengthening existing information security control environment
b) Comprehensive, well-structured approach to information security management means all relevant threats, vulnerabilities and impacts are more likely to be identified, assessed and treated rationally
c) Consistent approach to information risk management across all faculties, departments and business processes.
d) Cost savings on OBIS projects from standardisation of information security controls; avoids ‘re-inventing the wheel’ for each project
e) Cost savings through allowing OBU to concentrate effort and resources on specific additional security controls

f) Increased ‘brand value’ of OBU by achieving certification of a globally recognised and well respected security standard
g) A mechanism for measuring information security performance over time and incrementally raising quality
h) A coherent set of of information security policies, procedures and guidelines that are tailored to OBU and formally approved
i) Independent assurance of OBU’s information security management capabilities for staff, students, business partners, suppliers, regulators, auditors and other stakeholders.
j) Demonstration of senior management commitment to information security
k) An information security management system that is compliant with all existing data protection legislation and able to easily adapt to future changes
l) Information security management best practises that provide a valid defence in case of legal/regulatory enforcement actions following information security incidents

2.5 Constraints

By definition the design of the information management system for Oxford Brookes University is constrained by the documented ISO 27000 family of standards.

2.6 Interfaces

a) The ISO 27001 compliant ISMS will be implemented across all faculties and departments of OBU.
b) An independent, accredited, ISO 27001 assessment body will be appointed

2.7 Assumptions

a) Senior management will be supportive of adopting the ISO 27001 standard
b) The OBIS Information Management team will have sufficient time to carry out the required tasks of this project
c) The IT Information and Communications Manager will have sufficient time to carry out the required tasks of this project
d) Faculties and departments outside of OBIS will engage with the ISO 27001 compliance project and adopt all relevant information security controls (including all relevant policies, procedures and guidelines)
e) All faculties and departments will make staff available for internal audit visits
f) OBIS will make any necessary changes to technical information security controls (e.g. access control; asset management; change management; and encryption technologies)
g) EFM will be supportive of any changes to physical security controls that are necessary to ensure compliance with the ISO 27001 standard.
h) Third-party suppliers and contractors will adopt changes necessary to ensure OBU meets the requirements of the standard.

Customer Quality Expectations

a) The ISMS must be compliant with all clauses of the ISO 27001:2013 standard
b) The ISMS must be compliant with all applicable controls (as defined by the Statement of Applicability) in the ISO 27002:2013 standard
c) All policies, procedures and guidelines must be written in language appropriate to the relevant audience

d) All information security controls and requirements must be effectively communicated to all departments and faculties of OBU; all communications must demonstrate the reason for them and the benefits they bring.

3 Acceptance Criteria

a) The ISMS must be compliant with all clauses of the ISO 27001:2013 standard
b) The ISMS must be compliant with all applicable controls (as defined by the Statement of Applicability) in the ISO 27002:2013 standard

4 Outline Business Case

Capital:

Cost of independent certification (not due 'til 2018/19)
c. £15k to 20k for initial certification;
Project Costs:
Project Manager: 0.25 of time spent on project = 0.25 FTE @ £500 per day =~25k
External Training for Information Management Team - £1000 - One off cost
Conferences - 3 per year - £500 per conference = £1,500 per annum
Documentation - (the standard documents used for compliance) £500 - One off cost
Internal costs

- Employee: Per Annum
  - Head of Information Management - 0.4 FTE
  - Information Compliance Officer - 0.4 FTE
  - Information Management Officer - 0.2 FTE
  - Faculty and directorate staff (Including half day for internal audit visits)- 30-45 minute interviews for asset identification and business impact analysis @ 0.25 of the resources = 0.25 FTE @ £200 per day = 11k
- 10 people 1 day training = 2k

Maintenance:

ServiceNow - Control and Risk modules - ???
Cost of ongoing independent certification
c. £5k to £7.5k per annum for ongoing certification

Costs	2016/17	2017/18	2018/19	2019/20
Capital costs **- Cost of independent certification (not due 'til 2018/19)** **- Project Costs**	£28,000	£25,000	£32,000	£
Capital costs - Employees	£51,000	£51,000	£26,000	£
Running expenses	£	£	£	£
Technology	£	£	£	£
Maintenance and Support **- ServiceNow** **- Cost of ongoing independent certification**	£	£	£	£7,500 (ongoing per annum)
Other (e.g. Training, Data Load, Conversion, Backfill)	£	£	£	£
Contingency (20%)	£	£	£	£
Total cost of project	£	£	£	£

Total funding required (for costs not met by the service)	£	£	£	£

Financial Benefits	2016/17	2017/18	2018/19	2019/20
Budget savings	£	£	£	£
Income	£	£	£	£
Cost avoidance	£	£	£	£

Net Savings (benefits minus costs)	2016/17	2017/18	2018/19	2019/20
	£	£	£	£

5 Tolerances

Project to be completed by January 2019 with tolerance of +6 months.

Budget tolerance of +20%

6 Risks and Uncertainties

Risk & Description	Likelihood (1-5)	Impact (1-5)	Response Measure
There is a risk that this project will fail due to a lack of OBU senior management support caused by the project not engaging with its key stakeholders	1	5	Control: Clearly and succinctly define how this project benefits the University Have a communication plan which includes how to enhance stakeholder engagement at the appropriate times Clearly communicate benefits of ISO 27001 compliance to senior management and Brookes colleagues with roadshows as appropriate.

There is a risk that Brookes will fail to implement necessary security controls due to faculties and departments not delivering the work required caused by this project not being prioritised by OBU senior management	2	4	Control: Clearly communicated benefits of compliance to all faculties and departments Ensure senior management 'buy in'
There is a risk that changes to the current procedures will take too long to implement due a lack of 'buy in' from OBIs colleagues caused by to new procedures being more time consuming	1	5	Control: Early engagement with CTO, relevant OBIS managers and colleagues
There is a risk that we will not be able to change third parties contracts due to a lack of funding caused by the time and budget required to review and amend all current contracts	2	4	Control: Evaluate the need for specialist advice as part of the PID Ensure there is contingency budget for specialist legal advice
There is a risk that any new third parties contracts will not be compliant and therefore require changes due to legal oversight not considering ISO270001 caused by a lack of project and OBIS control	2	4	Control: Clearly communicate the requirements for new contracts to OBIS PMO and BPMs Ensure that the OBIS BPMs and the Information Compliance Office communicate to all University buyers
There is a risk that we may not achieve certification caused by incomplete work due to lack of time	1	5	Cotrol: Rolling timetable to ensure we conform to all controls by the end of the project

7 Customers, Users and Other Stakeholders.

a) All OBU staff, contractors and pseudo-employees that process data
b) OBU students
c) Independent ISO 27001 auditors