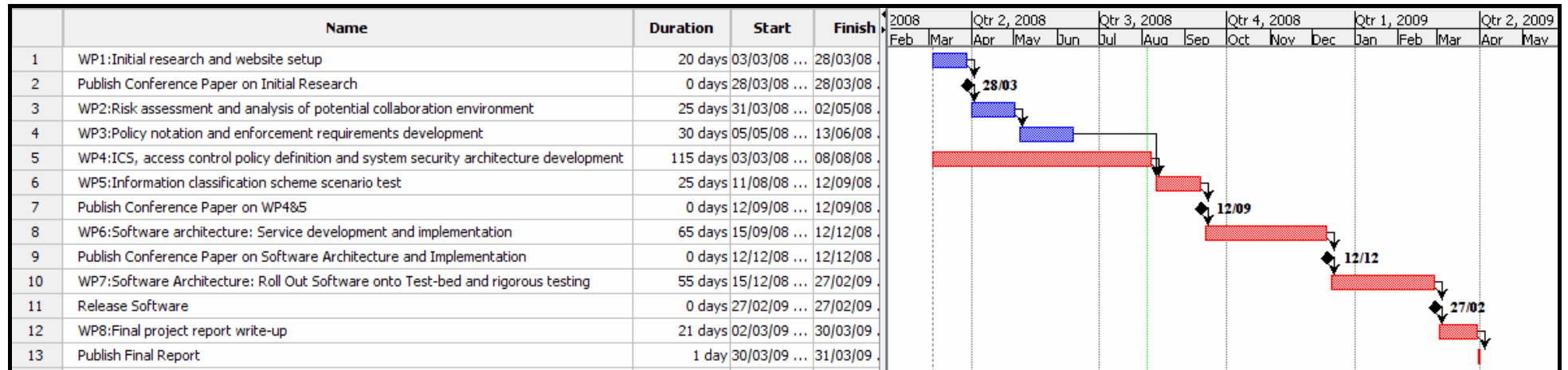




## JISC WORK PACKAGE



Project start date: 1<sup>st</sup> March 2008

Project completion date: 31<sup>st</sup> March 2009

Duration: 13 months

Workpackage and activity	Earliest start date	Latest completion date	Outputs (clearly indicate deliverables & reports in bold)	Milestone	Responsibility
<b>YEAR 1</b>					
<b>WORKPACKAGE 1:</b>					
<b>Objective:</b> The initial stage of the project will be to research current standards and technologies for data-level protection, the use of information classification schemes, and definition and enforcement of policy-controlled access to information – both at system level and the human readable level. The project team already has a research website and a domain will be set up on that site for the findings of this project.	03/03/08	28/03/08			
1. Identify and agree a set of specified subject areas for research, including but not limited to: <ul style="list-style-type: none"> <li>• Current standards and technologies for data level protection</li> <li>• Use of information classification schemes</li> <li>• Definition and enforcement of policy controlled access to information</li> </ul>					JH, PB, AT, RS
2. Identify relevant information sources to study related to subject areas					JH, PB, AT, RS
3. Acquire information from sources by carrying out research at each source					PB, AT, RS
4. Write paper on research findings			• <b>Project paper and report on findings</b>	<b>x</b>	PB
5. Set up a domain on the Cardiff and JISC websites for the project					PB
6. Set up PET Scanner project as a candidate for					JH

Workpackage and activity	Earliest start date	Latest completion date	Outputs (clearly indicate deliverables & reports in bold)	Milestone	Responsibility
study					
7. Post findings to project website (Cardiff & JISC)					PB
<b>WORKPACKAGE 2:</b>					
<b>Objective:</b> It is then proposed to undertake a risk assessment of the healthcare collaborative research environment in line with the PET scanner project currently underway at CU in order to understand the information security issues. An analysis of the risk assessment will identify the issues that can be effectively managed by existing security methods and identify those issues not addressed.	31/03/08	02/05/08			
8. Perform risk assessment of the healthcare collaborative research environment					JH, PB, AT
9. Produce a requirements specification for access control technology in VO research environments based on the risk assessment results			<ul style="list-style-type: none"> <li><b>Requirements specification for access control technology in VO research environments (document)</b></li> </ul>		JH, PB, AT
10. Perform gap analysis against existing security method capability based on the requirements spec					JH, PB, AT
11. Update website with the requirements spec					PB

Workpackage and activity	Earliest start date	Latest completion date	Outputs (clearly indicate deliverables & reports in bold)	Milestone	Responsibility
<p><b>WORKPACKAGE 3:</b></p> <p><b>Objective:</b> Early on in the project it will be necessary to develop a policy notation to enable the declaration of information protection requirements that is human and machine readable. This ensures the implementation of system-level security controls through policy bound to the data element. It is required early so that system implementation can begin early in the project cycle. Detailed policy can be specified in this notation later in the project to test the application of specific controls.</p>	05/05/08	13/06/08			
12. Perform research into existing information protection requirements notation					JH, PB, AT
13. Define a policy notation document based on the findings of the research, and the requirements specification from WP2			<ul style="list-style-type: none"> <li>• <b>Policy notation document</b></li> </ul>		JH, PB, AT
14. Define a policy enforcement requirement specification document based on the policy notation document and the requirements specification from WP2			<ul style="list-style-type: none"> <li>• <b>Policy enforcement requirements specification</b></li> </ul>		JH, PB, AT

Workpackage and activity	Earliest start date	Latest completion date	Outputs (clearly indicate deliverables & reports in bold)	Milestone	Responsibility
<b>WORKPACKAGE 4:</b>  <u><b>Objective:</b></u> Based on the security requirements specifications identified in WP 2 and 3, an information classification scheme and related protection needs will be defined. These needs will have access control policies defined, applicable both to human users and machine-readable system security policies. Following this study, a specification for a VO Security System will be defined. This will include a policy notation common to the platform and data elements.	03/03/08	08/08/08			
15. Perform research into existing information classification schemes and requirements					JH, PB
16. Define an appropriate information classification scheme and related information protection needs based on the requirements specified in WP 2 and 3, and taking into account the findings of the research in the previous task			<ul style="list-style-type: none"> <li>• <b>Information classification scheme requirements and definition document</b></li> </ul>		JH, PB
17. Define an access control policy that relates to the information classification scheme, in order that access restrictions could be applied to classified information			<ul style="list-style-type: none"> <li>• <b>Access control policy requirements and definition document</b></li> </ul>		PB
18. Define a scalable, dynamic VO security system architecture, unifying the policy notation, information classification, and access control policy			<ul style="list-style-type: none"> <li>• <b>VO security system architecture</b></li> </ul>		JH, PB, AT

Workpackage and activity	Earliest start date	Latest completion date	Outputs (clearly indicate deliverables & reports in bold)	Milestone	Responsibility
<p><b>WORKPACKAGE 5:</b></p> <p><b>Objective:</b> Whilst the system is being implemented (see WP 6), it is proposed to explore the transferability of the information classification scheme and associated controls to the medical research environment, particularly with respect to medical research results by applying it to a sample set of data from the PET scanner project. The aim is to both test the usability of the results as well as to develop a generic scheme that can be used by any organisation in a VO processing sensitive data.</p>	11/08/08	12/09/08			
19. Obtain a potential dataset of medical research results and understand the protection requirements of the information in situ, in transit, and in use					JH
20. Generate a storage, transfer and usage scenario for the dataset and apply the security system architecture defined in WP4 to the information					PB
21. Perform a risk assessment and hypothetical penetration test on the information to assess the usability, quality and effectiveness of the security system. Document the assessment in the form of an internal report and external paper.			<ul style="list-style-type: none"> <li>• <b>Report on usability, quality and effectiveness of the security system</b></li> <li>• <b>Conference paper on application of the information classification scheme and related controls to medical research information</b></li> </ul>	x	JH, PB, AT, RS

Workpackage and activity	Earliest start date	Latest completion date	Outputs (clearly indicate deliverables & reports in bold)	Milestone	Responsibility
<b>WORKPACKAGE 6:</b>  <b>Objective:</b> The system specification will be implemented using a service-oriented architecture, utilising web services, policy definition and user identity standards and related technologies, and latest security infrastructure. The system will be developed with an underlying distributed architecture to provide an alternative to the more common approach of centralised user management and security control.	15/09/08	12/12/08			
22. Develop system architecture to support the implementation of the VO security system architecture defined in WP4. Write up concepts and structure of the architecture in the form of a conference paper			<ul style="list-style-type: none"> <li>• <b>Conference paper on the system architecture and comparison to existing architectures that do need meet the requirements of collaborative VO information sharing to such a fine granularity.</b></li> </ul>	x	PB, AT, RS
23. Develop services to implement each part of the system architecture					PB
24. Implement each service until each part of the system architecture is deployed					PB
25. Fully integrate the deployed services and create a fully operational solution based on the initial VO security system architecture.			<ul style="list-style-type: none"> <li>• <b>Software implementation of the proposed system architecture for demonstration and dissemination.</b></li> </ul>		PB
26. Write up the results of the implementation into a journal paper			<ul style="list-style-type: none"> <li>• <b>Journal paper on the complete solution to include the initial research, analysis and risk assessment of VO research environments, information</b></li> </ul>	X	PB

Workpackage and activity	Earliest start date	Latest completion date	Outputs (clearly indicate deliverables & reports in bold)	Milestone	Responsibility
			<b>classification scheme and policy notation, and software implementation</b>		
<p><b>WORKPACKAGE 7:</b></p> <p><b>Objective:</b> The implementation of the technical solution would then be installed onto the test-bed machines to provide a live test scenario and initial performance results. By setting up several back-end machines hosting various information resources, all of which have the access control policy applied to them, the access control mechanisms can be enforced by attempting to access the resources through the software installed on the client machines. UCISA and ENISA will be invited to submit information of their own to the test-bed to provide additional results and proof of concept. We also consider testing the robustness of the prototype, in the first instance, by offering a challenge with CU's School of Computer Science to see if anybody can crack the security. Subsequently we may offer the same challenge to members of the Jericho Forum. The software will be fully documented with FAQ, installation guide and distributed with the initial test results. Guidance will be taken from the Open Source Maturity Model, and the senior researcher on the project has previous experience with the quality assured development of software for the OMII.</p>	15/12/08	27/02/09			
27. Define test-bed machine configuration and information distribution					PB, RS

Workpackage and activity	Earliest start date	Latest completion date	Outputs (clearly indicate deliverables & reports in bold)	Milestone	Responsibility
28. Generate and store test-bed data from PET scanner, UCISA, ENISA and any other willing sources using the information distribution configuration define in the previous task					PB
29. Roll out the software from WP6 onto the test-bed machines					PB
30. Apply information classification scheme and protection requirements to information					PB
31. Define access control policy for the information					JH, PB, AT
32. Define a set of usage and penetration tests to rigorously test the effectiveness and robustness of the deployed software					JH, PB, AT
33. Invite other parties to perform usage and penetration tests					JH, PB, AT
34. Fully document and define FAQ for the software, develop an installation guide and distribute with the initial test results			<ul style="list-style-type: none"> <li>• <b>Release (under licence) of the first version of the software including documentation</b></li> <li>• <b>Presentation/Demonstration of the software internally at CU, to UCISA, to the Jericho Forum members, and to ENISA.</b></li> </ul>	<b>X</b>	PB
35. Develop a report on future development requirements and bugs for the software			<ul style="list-style-type: none"> <li>• <b>Report on future development requirements and bugs</b></li> </ul>		PB

Workpackage and activity	Earliest start date	Latest completion date	Outputs (clearly indicate deliverables & reports in bold)	Milestone	Responsibility
<b>WORKPACKAGE 8:</b>					
<b>Objective:</b> The final work package will see the end of the project, but after the various papers and particularly, the demonstrations to CU, UCISA, Jericho Forum and ENISA, the project will be sustainable through integration into any one (or more) of the enterprise architectures of these organisations or by sale under licence to other organisations. The final report to JISC will be the end of this funded work, but the agenda at CU is to push the resulting theories and software into the academic and commercial domains.	02/03/09	30/03/09			
36. Write final project report			<ul style="list-style-type: none"> <li><b>Final Project Report</b></li> </ul>	X	JH, PB, AT, RS
37. Ensure all papers and reports are uploaded to website			<ul style="list-style-type: none"> <li><b>Conference and Journal papers, once published will be published on the project web site</b></li> <li><b>Publication of all related work to website (ongoing)</b></li> </ul>		PB
38. Disseminate case study through all available routes					JH, PB, AT, RS
39. Disseminate contact details with all publications					PB

Members of Project Team:

PB = Pete Burnap  
JH = Jeremy Hilton  
AT = Anas Tawileh  
RS = Rhys Smith

Workpackage and activity	Earliest start date	Latest completion date	Outputs (clearly indicate deliverables & reports in bold)	Milestone	Responsibility
--------------------------	---------------------	------------------------	--	-----------	----------------

1: Initial research and website setup
2: Risk assessment and analysis of potential collaboration environment
3: Policy notation and enforcement requirements development
4: Information classification scheme, access control policy definition and system security architecture development
5: Information classification scheme scenario test
6: Software architecture: Service development and implementation
7: Software Architecture: Roll Out Software onto Test-bed and rigorous testing
8: Final project report write-up