|  |  |
| --- | --- |
| **Title** | Access Control in Multi-Tenant Cloud Environment |
| **Student name:** | Stephen Hart |
| **Supervisor name:** | Dr Anna Lisa Ferrera |
|  | |
| ***Aims/research question and Objectives*** | |
| **Project Aims**  The main aim of the project is to create an access control model that can be used by tenants within the same IaaS provider to share data securely and meet data protection legislation.  **Project Objectives**  The objectives are of the access control model:   1. Meet the requirements for the UK Data Protection laws. 2. Comply with the new EU Data Protection legislation: “GDPR (2016), General Data Protection Regulation, (EU) 2016/679”. 3. Document the migration process to move data from Discretionary Access Control (DAC) where the data is stored in an NTFS (New Technology File System) on a Microsoft Windows server. 4. The administrator can set access control at a granular level based on several attributes of the object (data) and attributes of the user. 5. Where non-human process needs to access data across tenants this can be done by attributes to the service account used by the process. 6. Document the model and how access rights are assigned and can be revoked.   **Research Question Motivation**   * General Data Protection Regulations (GDPR)   In 2018, new European data protection laws, General Data Protection Regulation 2016 (GDPR) come into effect. Organisations can’t simply try to keep all its data in a single location. New regulations have significant fines for non-compliance and apply to any organisation in the world holding any EU citizen data.   * Increase Cyber Attacks   “*2015 saw the biggest increase in cyber-attacks in over ten years*”, PwC survey (2016).  Opportunity to improve security and reduce risk and mitigation of a cyber attack, without companies feeling losing control over their critical data.   * Move to Public Cloud Infrastructure as a Service (IaaS)   “*5,000 Exabytes data created every year and transmitted in Europe by 2020 a growth of tenfold* “, survey by EMC and IDC. This will increase the risks to non-compliance of data protection without the appropriate access controls.  **Possible Outcomes**  The outcome could be a access control solution that could meet more complex data sharing requirements in an IaaS cloud environment. | |

|  |
| --- |
| ***Summary of proposed research and analysis methodology*** |
| **Problem**  At the start of the project it is not known how much support will be provided by the cloud vendor or if it is possible to setup the environment on the Southampton University infrastructure. Where the project finds a vendor, who is willing to assist in the project the time they are willing to support the project may be limited. However, it is also possible that cloud vendor support may not be required as the model can be built from publicly available services used as a free trial period or paid services.  **Design Approach**  The proposed design approach is to research and plan as much as possible before the build stage, as to limit the time required from the cloud vendor or Southampton University support team or reduce costs of any paid services. The design stage will include creating the test plans.  It is proposed for the build stage to use a Rapid Application Development methodology (RAD), see figure 1 below.    Figure 1 – Rapid Application Development (RAD) – See PERT Chart  The RAD approach will limit the time required from cloud vendor support for the build stage and/or costs for paying the cloud vendor if not using free trail or free support from the vendor.  **Reproducibility**  It is intended to document the setup of the cloud environment so it can be reproduced. Where for example costs reasons features such as two-factor authentication can’t be setup in the model but will be described in the documentation.  Not all project objectives may be verified by the prototype access model and alternative verification method that the prototype can meet the objective may be required.  **Testing**  Literature review of comparable projects will be completed to find any methodologies that can be reused.  **Summary**  It is not known what support will be given by the cloud vendor (and if required) and the project methodology will be run to limit the time required in build and testing stages, however not all project outcomes may be verified in the model so alternative verification may be required. |

|  |
| --- |
| ***Research plan – Gantt chart or Pert chart*** |
| **PERT Chart**    **Comments / Other Tasks**   * Total project length 14 weeks * Draft report to be regularly updated * RAD stage may be iterative but no longer than five weeks * Weekly meetings with supervisor * Feedback results to any vendor who assisted in the project |

|  |
| --- |
| ***Ethical statement*** |
| **Data Protection**  This project is to provide an access control model in a IaaS multi-tenant cloud environment and could be based on:   * Support from a cloud vendor; * Use of free trial and paid cloud vendor services.   An alternative to the above two options is the possibility that it could be hosted on Southampton University Infrastructure, although not expected this option to be taken.  The data used will not be real data so outside of the scope of the Data Protection legislation, however some of the users of the model may be using real names and could be identifiable. To ensure no data protection breach it is proposed that:   * all data will be securely deleted at the end of the project; * all users who use the system sign agreement not to load data that would be in scope of Data Protection legislation   **Licensed Software**  The project will be using licensed software and the project lead will be responsible to ensure any software installed or used is:   * Used within the agree license terms of agreement * Installed within the license terms of agreement * Uninstalled at the end of the project and any copies of license key numbers handed back and copies destroyed * Record kept of all licenses used, including any relevant information such licenses keys * Any software media is handed back at the end of the project   **Policies**   * Lone Worker Policy   The project will not require a lone working policy as no one will be left alone in data centres or other work areas.   * Code of Ethics   The project lead is a Certified Information Systems Security Professional (CISSP) certified by ISC2 and as such will follow the ISC2 Code of Ethics <https://www.isc2.org/ethics>. |

|  |
| --- |
| ***Legal and commercial aspects*** |
| **Commercial**  It is not intended that the project will produce any intellectual property as all software used in the project is commercially available. However, when working on site in data centres anyone working on the project will need to comply with confidentiality and sign non-disclosure agreements as required if working on company premises and particular in any data centres.  **Legal**  Agreement with any commercial organisation on sharing outcomes of this project must be agreed before starting engagement. The testing of the access control model will not include any vulnerability tests of the cloud infrastructure environment, unless with clear written permission of the cloud vendor and following any change control procedure as required.  Health & Safety at Work Act 1974 will apply working at Southampton University and if working on any vendor site the project lead must ensure any project team member reads the relevant health & safety risks assessment before entering areas for example data centres because of the possible risks involved in working in these as working in confined spaces alone in area that may have gas drenching system will be a higher risk than normal office environment. |