

PROJECT DOCUMENTATION

FEASIBILITY BUSINESS CASE

Marches Centre for Cyber Security

Release: Draft

Date: 12.06.18

Author: Mark Pearce

Document Number: V1.0

Feasibility Business Case History

Document Location

This document is only valid on the day it was printed.

The source of the document will be found at Economic Regeneration / Enterprise Zone G Drive

Revision History

Date of this revision: 12.06.18

Date of next revision:

Revision date	Previous revision date	Summary of Changes	Changes marked
12.06.18	n/a	First issue	n/a

Approvals

This document requires the following approvals.

Name	Signature	Title	Date of Issue	Version

Distribution

This document has been distributed to

Name	Title	Date of Issue	Version	Status
CSWG		12.06.18	V1.0	Draft

Table of Contents

1.	Purpose of Document	6
2.	Objectives	6
3.	Background	6
3.1.	Project Drivers and High Level Issues	6
3.2.	High Level Metrics	6
4.	Scope.....	7
4.1.	Included in Scope.....	7
4.2.	Not included in Scope	7
5.	Stakeholders	7
6.	Dependencies	7
6.1.	Initiatives which depend on this project are:	7
6.2.	This project depends on:	7
7.	Benefits	8
7.1.	Quantifiable	8
7.2.	Non-quantifiable.....	8
8.	Contribution to Strategic Objectives.....	8
9.	Potential Costs and Options for Project.....	8
10.	Costs and Timescales to Develop the Full Business Case	9
11.	Risks of not doing the Project	9
11.1.	The key risks of not doing the project are:	9
11.2.	The key project risks are:	10
12.	Appendices	10
	Appendix 2 – Equality and Diversity considerations	10
	Appendix 3 – Privacy and information security considerations	10
	Appendix 4 – Sustainability considerations.....	10

Stage 0 Business Case

1. Purpose of Document

This Feasibility Business Case contains information that describes the justification for setting up and continuing the development of a detailed Business Case for Marches Centre for Cyber Security project. The Business Case is to be submitted to the Capital Strategy Working Group / HEZ Capital Project Board and if accepted, a more detailed Business Case will be developed.

2. Objectives

This project is designed to provide a unique set of facilities and services to foster and catalyse the development of the local cyber centre and generate cyber resilience amongst Marches businesses and institutions.

3. Background

3.1. Project Drivers and High Level Issues

The UK is a market leader in the cyber security sector. This is a multibillion pound and fast growing market. A Science and Innovation Audit (about to be concluded) reinforces Herefordshire's position (as part of the Cyber Valley with Worcestershire, Gloucestershire and Swindon) as an important location for cyber businesses, not least the proximity to, and the spin off from, the SAS (and signals) in Hereford; Qinetiq in Malvern and GCHQ in Gloucester.

The University of Wolverhampton has a longstanding interest in the cyber sector. It has recently created a Cyber Research Institute to increase its investment in cyber research, particularly in key sectors and infrastructure. The University has researched the market extensively and has articulated the potential growth in cyber. In addition to research areas including cyber specialist product and services companies, embedding cyber resilience in key supply chains and institutions, providing expert and certified education and training. Accordingly, the University has developed a proposition for a new facility incorporating these features and, given the profile and importance of the sector locally, and the business ready support and profile provided by the Hereford Enterprise Zone, want to locate it on Skylon Park.

3.2. High Level Metrics

1,000 sqm of research and development space

1,500 sqm of employment space

250 sqm of training space

16 businesses housed

15 FTE jobs in the Centre, 175 FTE jobs in businesses

4. Scope

4.1. Included in Scope

It is proposed to develop a Centre for Cyber Security located on the Hereford Enterprise Zone. The proposed centre will form part of a 'Cyber Triangle' with GCHQ Cheltenham and Malvern Hills Science Park. It will be an anchor building generating new research opportunities and enhancing the student experience through the application of applied research and knowledge transfer partnerships which will:

- stimulate a base of SMEs engaged in cyber-security solutions
- drive up levels of innovation activity in the cyber-security
- improve insight on cyber-security challenges and opportunities for SMEs across the Marches.

The building will comprise the following spaces:

- office/workshops/laboratories for cyber related tenant companies and incubation space for start-up companies
- advanced facilities for University and partners cyber space research development and commercialisation of intellectual property
- secure training rooms for the delivery of University short courses and educational programmes

all co-located under one roof in a specialist facility which will be a focal point for cyber-security activity and defence /security related businesses.

The centre will provide innovation workspace for small and start-up businesses to operate from. These facilities will provide ready access to consultancy support from the University and shared facilities including lab space and training rooms. The combination of support, facilities and co-location with potential collaborators will significantly enhance the environment for investment and enterprise. It will contain specialist facilities for the cyber sector including server space, very high speed broadband, as well as R&D lab space. The physical fabric of the building will offer the high levels of security for data transmission and storage which will ensure Skylon Park attracts a growing base of cyber-related businesses and activity.

The centre will offer training to SMEs and other organisations on cyber-security issues. Courses will range from basic Cyber Bytes and Cyber Essentials (for all businesses on line) through to highly specialist programmes on cyber security for the police, defence and financial services businesses.

The building will provide users with access to space and support, connections, knowledge, experience and investment through:

- Over 1,000m² of R&D floor space for 3 cyber laboratories, providing new laboratory and testing facilities for researchers in this area.

- More than 1,500m² of employment space for 16 cyber security business incubator units, 2 workshops and 3 high security meeting rooms
- 250m² of high quality secure business training floor space

The fabric of the building will contain a physical security firewall between all major elements of the building and a secure server room.

The key partners in the development are intended to be the University of Wolverhampton, Herefordshire Council and QinetiQ. The Centre is intended to be a joint venture between the University of Wolverhampton and Herefordshire Council.

The planned activities to be undertaken within the Centre for Cyber Security will comprise:

- Research & Knowledge Transfer
- Incubator and tenant companies
- Training programmes delivery

The key research and development partner will be QinetiQ which is a British multinational defence technology company headquartered in Farnborough with a site in Malvern. It is the world's 52nd-largest defence and the sixth-largest based in the UK. It is the part of the former UK government agency, Defence Evaluation and Research Agency (DERA), which was privatised in June 2001. The partnership with QinetiQ will allow the University access to an £80 million Cyber Range (one of only 6 in the UK), which will allow researchers, students and businesses unprecedented access to sophisticated simulation and emulation cyber test-bed platforms.

University researchers and students will have unique access to the Cyber Range and will be able to simulate cyberattacks and cyber mitigation strategies. This will benefit and inform research, and help develop informed curriculum.

Access for businesses to the Cyber Range will be a unique feature of the Centre and will allow organisations to test and validate new products in a secure and regulated environment.

4.2. Not included in Scope

Development outside the Cyber Centre boundary

5. Stakeholders

The University of Wolverhampton are leading on the development of the project and are liaising with businesses and institutions to further that development.

In terms of the development of the business case to support the project, we will need input via the EZ Capital Works Programme Board from legal, finance, governance.

The Cabinet member and related Member interests will need to be informed/involved.

Hereford Enterprise Zone Board are championing land usage at the EZ.

6. Dependencies

6.1. Initiatives which depend on this project are:

None

6.2. This project depends on:

Timely governance decisions on Council support and the nature of that support, in particular the input from various services to enable those decisions to be taken.

It requires the University of Wolverhampton as the lead on the project to follow through its own governance arrangements in a timely fashion to confirm the budget and implementation arrangements as above.

7. Benefits

7.1. Quantifiable

1,000 sqm of research and development space

1,500 sqm of employment space

250 sqm of training space

16 businesses housed

15 FTE jobs in the Centre, 175 FTE jobs in businesses

5SMEs created. Student placements, graduate employment, IP licences, Knowledge Transfer Metrics, and numbers trained/certified Metrics all to be part of the detailed business case.

7.2. Non-quantifiable

Add a unique mix to the asset-base for Hereford and the Cyber Valley area

Add impetus to the development of high value added businesses and jobs on the Zone

Add profile to the inward investment offer for the Zone and Herefordshire, improving opportunities to bring in businesses to base themselves or make use of the facilities.

8. Contribution to Strategic Objectives

Herefordshire Corporate Plan 2016-20

- Develop and start the implementation of a countywide Economic Masterplan: The Cyber Centre is a priority project within the Masterplan/Economic Vision and delivery it will contribute to the implementation of the plan
- Finalise and implement plans that strengthen and diversify the economy of Herefordshire: The Centre aims to support the creation and growth of businesses within the cyber sector a local business strength and embed resilience in fast growing businesses, improving productivity and innovation
- Make Herefordshire more attractive to younger age groups, for a more balanced age profile, improving local access to skills, training so that everyone can benefit from economic prosperity. The Centre focusses on a high growing sector requiring IT skills, providing an opportunity for younger people to train and grow careers locally.

9. Potential Costs and Options for Project

The University of Wolverhampton has developed the concept based on market needs and shaped the design based on direct best practice that it operates elsewhere. The University has invested in a detailed RIBA Stage 3 design and cost plan which has established the building cost at £9m. The EZ MD is part of the Steering Group for that development and has had full access to the cost plans and the analysis and tests, using direct construction experience from the University as benchmarks.

The Centre concept and design has been accepted by the Marches LEP and ESIF.

The University has secured £4.1m grant funding, £2.8m from the Marches LEP and £1.3m from ESIF.

The University is also conducting detailed business planning for the operation of the Centre – this sees a surplus once the Centre is fully established – even under worst case scenario.

The University is now seeking investment from the Council as follows:

£2.0m as short term borrowing

£1.5m as equity)	
)	£2m in total
£0.5m plot land value as equity)	

Total project value £9.5m

The terms of the loan (rate and duration) to be determined.

The terms of the investment (expected return etc) also to be determined (see above)

10. Costs and Timescales to Develop the Full Business Case

Wolverhampton University have prepared draft HoTs for the engagement with Herefordshire Council. The University wishes to create a JV company with the Council, with shares proportionate to the level of investment made.

The University is also preparing a business plan with financial scenarios for the operation of the Centre.

The University would like to be on site by January 2019, which means going through the contractor tender process in the autumn.

Input will be needed from legal and finance in particular to advise on the HoTs and jv arrangements, and review the business plan in order to inform the business case.

The principle of engagement with the University and the scale of input needs to be taken through the Council's governance process. This will likely frame the timetable above.

11. Risks

11.1. The key risks of not doing the project are:

RISK: lack of facilities and services means cyber businesses choose to move elsewhere to set up and grow

RESPONSE: Seek to try to encourage the growth of the local sector through virtual means

11.2. The key project risks are:

RISK: Terms of engagement with the University of Wolverhampton do not meet the Council's governance, financial and legal requirements.

RESPONSE: Council to input and agree Heads of Terms, any Company structure and Business Plan for the project.

RISK: Cost of project exceeds the budget

RESPONSE: Independent design and cost plan prepared and reviewed regularly – tested through open tender. University to absorb any potential increases either through design modification or contingency.

RISK: Centre generates less revenue than anticipated impacting on the viability of the Centre and returns to the Council

RESPONSE: In depth market analysis and testing undertaken by the University. Reinforced by the independent SIA. Key resource to be identified in advance to develop and implement a marketing plan and pilot activity [University to guarantee return to Council?]

RISK: Centre fails to deliver outputs

RESPONSE: As above.

12. Appendices

Appendix 1 – Finance Template (template available)

Appendix 2 – Equality and Diversity considerations

This appendix should contain the assessment of any Equality and Diversity considerations, if any are known at this point.

Appendix 3 – Privacy and information security considerations

This appendix should contain the assessment of any Privacy and Information Security considerations, if any are known at this point.

Appendix 4 – Sustainability considerations

This appendix should contain the assessment of any Sustainability considerations, if any are known at this point. It may be possible to do an initial Sustainability Impact Analysis to judge how sustainable the project is likely to be (though this is not essential at this stage:

	+ve	-ve
<i>Environmental</i>	<i>e.g. Energy savings Transport savings Paper savings</i>	<i>e.g. Additional Energy costs Transport costs Paper costs</i>
<i>Social</i>	<i>Benefits to:</i> <ul style="list-style-type: none"> - <i>Individuals</i> - <i>Stakeholders</i> - <i>Council</i> - <i>Local Community</i> 	<i>Potential issues and adverse effects for:</i> <ul style="list-style-type: none"> - <i>Individuals</i> - <i>Stakeholders</i> - <i>Council</i> - <i>Local Community</i>
<i>Economic</i>	<i>Potential increases to revenues Reduction of financial risk Future cost savings</i>	<i>Software costs (initial and ongoing) Storage costs Additional staff costs</i>

Once the analysis is done it should be considered what actions would minimise the negative column and increase the positive column and those actions could be recorded in this appendix.