The Power of Information – Threats and Opportunities in Defence Export Control

Joe G Dunn[1], Carsten Maple[2], Gregory Epiphaniou[2]

[1]WMG, University of Warwick, Coventry, UK & BAE Systems plc, Farnborough, UK
[2]WMG, University of Warwick, Coventry, UK

Keywords: Export Control, Consent Agreement, IT Automation, ITAR, Cyber Security

Abstract

In Security and Defence, adherence to complex Export Control legislation is essential. For Governments, it is necessary to ensure that regulated items such as hardware, technical data, and defence services are only exported to authorised users. For Companies, it is vital that they comply with the applicable laws of all the countries concerned; otherwise, they can be fined or ultimately debarred, losing their 'licence to trade'.

Driven by the accelerated use of Information Technology, the risk balance has transformed from risks largely concerned with unlicensed hardware to now being centred on information risks. Recent cases highlight that the majority of alleged violations contain information assets. In tandem with this threat, opportunities have arisen since these information capabilities have also produced toolsets to help risk mitigation.

This paper is based on research undertaken in support of an Export Control IT Automation programme. The methodology commenced with a Literature Review that included a detailed analysis of the allegations and the remedies reached for all US Department of State cases where a Consent Agreement was used to settle alleged Export Control violations. These include non-US Companies, as US Export Controls are applied extra-territorially.

This work distils into themes the issues that have been encountered, and contains process-steps and measures that can be taken to mitigate risk. The findings also discuss the identified risks associated with managing Export Controlled information, and the types of IT Automation toolsets available to mitigate these risks.

The work should be of interest to all parties involved in Export Control.

1. Introduction

Export Controls exist to prevent the export of defence articles and defence services including technical data to unlicenced countries, thereby supporting, amongst other items, the foreign policy objectives of the exporting countries. US Export Control legislation is complex and applies extra-territorially i.e. to exports from the US and to subsequent re-exports from recipient countries. Export Control compliance demands have increased over the years and this paper utilises an analysis of agreements, known as Consent Agreements, entered into to settle alleged violations. This paper studies the various risks that exist and the shift that has occurred from a primary hardware focus, to a focus on information in the form of Technical Data. Information risks are harder to mitigate than the hardware risks due to the nature of information, and the ease with which it can be replicated, accessed, and transmitted.

Export Controls can be complex, especially for multi-national products. Consider the example of the Eurofighter Typhoon airframe, as represented in Figure 1. As depicted the major assemblies that comprise the completed airframe are sourced from the Eurofighter Partner Companies (EPCs) in the four nations. Each country is accountable for the assembly and equipping of the major units shown. Final assembly of the airframe is then performed at the final assembly line associated with the customer for the end product. From an Export Control perspective, all Export Controlled equipment forming part of the units to be shipped needs to be licenced for the physical assets.

Figure 1: How to build a Typhoon workshare (Source [1])

In the case of US Export Controlled items, this could involve several Export Control transactions, for example:

1. Export of equipment for inclusion into a major assembly.
2. Re-export of equipment as an integral part of a major assembly to the destination of the final assembly line.
3. Re-export of equipment as part of the aircraft to its final customer destination.

This example, although complex, deals with tangible assets such as airframe equipment. Additionally, as will be explored in this paper, the Export Control of information in the form of Technical Data represents a much greater challenge and contains harder risks to mitigate.

This paper describes the mechanisms associated with the Consent Agreements, the various risks identified, including information risks and the expectation that IT Automation will be used to mitigate these risks.

The remainder of this paper is structured as follows: Section 2 provides some essential background on US Export Control legislation and the Consent Agreement mechanism. Section 3 describes the method employed. Section 4 presents the research results and a discussion. Additionally, Section 4 proposes four main periods of Consent Agreements. It also describes the shift of emphasis from hardware to information. Therefore, hardware remains important but is augmented by management of information. The section then describes the information risks that have been identified from the analysis along with key Information Technologies that can be used to mitigate the risk. Finally, Section 4 identifies those technologies that the authors plan to explore in future work and introduces some generic process steps to minimise risk – again a focus of further development work. Section 5 discusses the limitations of this work and, finally, Section 6 concludes the paper.

2. Background

Typically Export Controls are governed by the country from which the goods and / or services are being exported. US Export Control laws differ in that, in addition to applying to exports from the US, they are also applied 'extra-territorially'. So, for example, if defense articles or services including Technical Data are exported from the US to the UK and then onwards to another country, then both UK and US laws apply to the last export transaction.

This paper highlights key aspects and conclusions from an extensive literature review, currently in preparation for publication, which was conducted across all documentation associated with Consent Agreements from their inception in this area, through to the most recent ones in 2021. The information is all in the public domain and is accessible from documents linked through [2].

Some limited background on US legislation is required to understand the context of this work. Two key areas of regulation are used to enact the US Export Control legislation, namely:
1. The International Traffic in Arms Regulations (ITAR). These are governed through the US Department of State (US DoS) and specifically the Directorate of Defense Trade Controls (DDTC). The ITAR applies to all defense articles and defense services as featured on the US Munitions List (USML) [4].
2. The Export Administration Regulations (EAR). These are governed by the US Department of Commerce (US DoC). The EAR applies to 'Dual Use'[1] items as covered on the Commerce Control, List (CCL). [5].

[1] Dual Use items refers to items with military and commercial end uses. E.g. A missile would be an example of a military item, whereas a radar could be dual use.

Further information on US regulations may be found in [6] and [7], with a good summary paper on ITAR available at [8].

The Consent Agreement is a mechanism used to settle violations or alleged violations of the ITAR. In this context Consent Agreements are defined as shown in Figure 2 below.

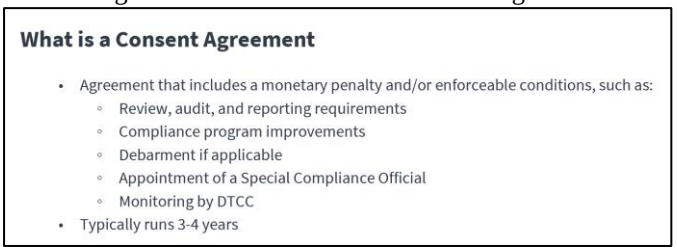

Figure 2 What is a Consent Agreement (Source Ref [3])

The structure of the documentation surrounding these agreements has, since Consent Agreement number 6, generally followed a standard pattern of:

1. Proposed Charging Letter (PCL)
This sets out the alleged violations and is written from the DDTC to a senior executive of the company responsible for the alleged breaches.
2. Consent Agreement
This sets out the legally binding agreement including all the measures that need to be enacted. It is signed by the parties entering into the Consent Agreement, namely the DDTC and the company responsible for the allegations.
3. Order
This is the Order that legally enacts the Consent Agreement and is issued by the DDTC.

All three documents within this set are published and available on the DDTC website [2]. There is little information on the subsequent actions used to close out the Consent Agreements' commitments.

3. Method

The method used for this work is as represented in Figure 3.

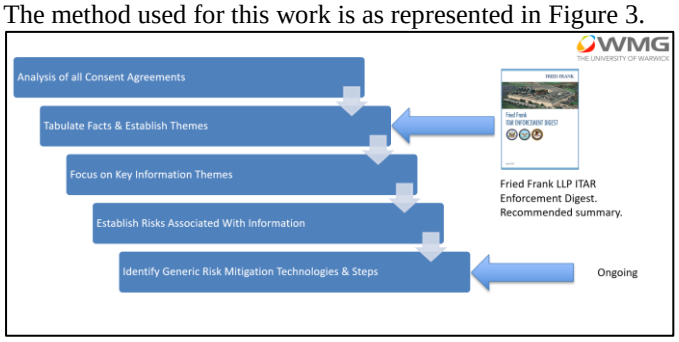

Figure 3: Schematic Representation of Method (Note: ITAR Enforcement Digest is at Ref. [9])

As shown in this figure, the starting point was to perform a Literature Review, currently in preparation for publication, which included the need to read, digest and analyse the documentation associated with circa 60 Consent Agreements

(over 1,500 pages) that have been entered into since this mechanism's inception. The next task was to tabulate the facts, including fines, terms, nominal duration, and then analyse the agreements for themes. This work included understanding the various mechanisms that are used to enforce the agreement, analysing how these had developed through time and proposing key themes. One of these themes that was further developed was that of information as both a risk (i.e. part of the alleged violations) and the growing expectancy that Information Technology toolsets would be used to mitigate these risks. During this analysis, an excellent reference source was discovered - the ITAR Enforcement Digest [9], produced by the legal company Fried Frank LLP. The research work presented in this paper differs from the digest in the following ways:

1. It covers the period prior to 2001 and post January 2020,
2. It develops themes and especially ones relating to risks and especially information risks.
3. It charts the increasing expectation that evermore sophisticated IT Automation solutions will mitigate these risks.

Nevertheless, the digest [9], is highly recommended as a summary condensing over 1250 pages of documentation into a 96 page document.

The method then specifically took the risks outlined and identified Information Technologies that could be used to mitigate these risks, and commenced work on developing generic process steps.

4. Results & Discussion

4.1 Results & Discussion 1 – General Themes

One of the key mechanisms used in Consent Agreements is that of a monetary fine. As shown in Figure 4, these fines significantly increased in the early 2000s. From the late 1990s in some cases it was possible for part of a fine to be suspended (e.g. 25%) and for this to be applied to compliance improvements specified in the Consent Agreement. The actual percentage varies by case, is written into the Consent Agreement, and is also subject to audit.

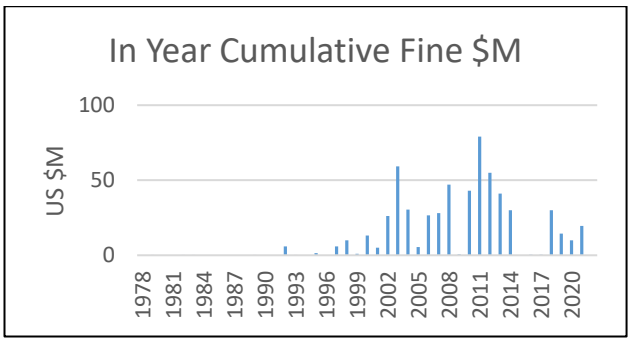

Figure 4: Consent Agreement Fines (Based on material in Source Ref [3])

Whilst the monetary fines are often the headlines reported (see [10], for a recent example) other mechanisms are used, and these are summarised in Figure 5.

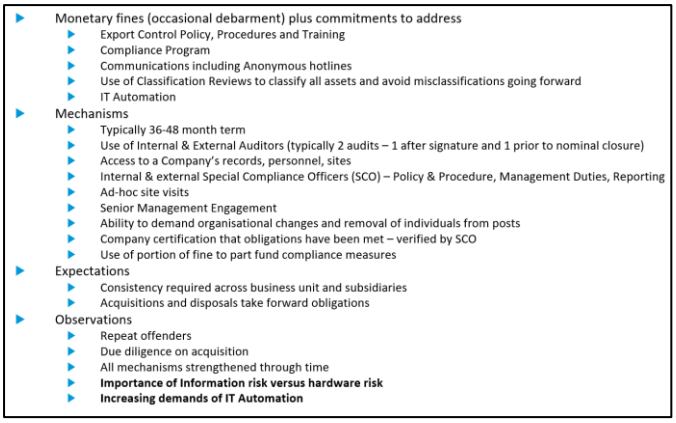

Figure 5: General Themes

The complete discussion of these mechanisms and how they have been developed and strengthened over time will be covered in the complete Literature Review and is too extensive for inclusion in this paper. A good view of the current use of these mechanisms can be gained by reading a recent Consent Agreement such as that at [11].

An expectation that is worth noting, especially for more complex organisations, is that any measures are presumed to be applied across all relevant business units and subsidiaries. Also, in the event of a business unit acquisition, the obligations apply to the new acquisition. Conversely, in the event of a disposal, the obligations pass forward to the new ownership.

Another observation was that 'repeat offenders', especially ones where previously committed-to obligations have not been implemented, were reprimanded.

It should be noted that due diligence performed as part of a company acquisition was often the trigger for discovery of alleged violations.

Finally, the importance of information as a risk that has grown though time and the expectation of using IT Automation tools to mitigate this risk will be discussed in the next sections.

4.2 Results & Discussion 2 – Summary Timeline

Having analysed all Consent Agreements, this research proposes the broad periods as illustrated in Figure 6. These periods are not 'hard and fast', and there will be some characteristics of a case in one period that overlap into another one. However, they have a value in describing the general themes that have developed over time, especially regarding the information theme. Each period builds upon the previous one so by the time, for example, Period 3 is reached, it is not suggesting that hardware is unimportant. Instead the previous demands have been built upon, and the important consideration of Information Security has been added, as highlighted in cases within that period.

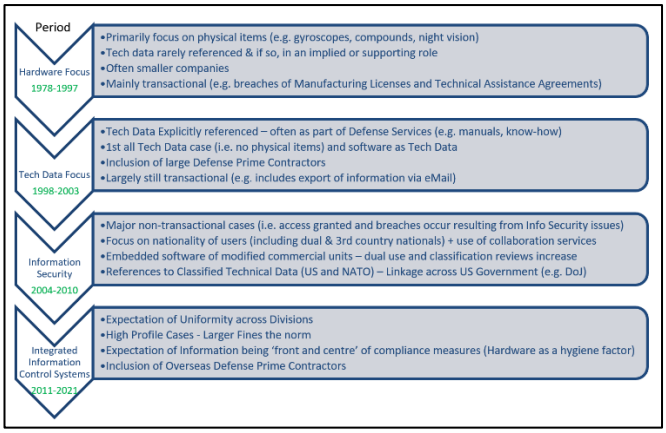

Figure 6: Proposed Four Periods of CAs (Based on analysis of data in Ref. [2])

A brief description of the illustrated periods now follows.

1. Hardware Focus (1978-1997)

As shown in the figure, these early cases were primarily concerned with the export control of hardware. Technical Data is rarely referenced, and when it is, it is usually in a supporting or an ambiguous way (e.g. quoting that the law prohibits the export of Technical Data but not referencing specific allegations). These cases were also largely transactional and often involved smaller companies.

2. Technical Data Focus (1998-2003)

This period commences with the first case to explicitly reference Technical Data as a major part of the allegations [12]. It also includes the first case chiefly centred on Technical Data and Defense Services [13] and the inclusion of software as a piece of Technical Data in the allegations [14]. As with the first period, the focus of these cases remains transactional e.g. shipping of hardware or Technical Data, with the latter being done physically or electronically e.g. via eMail. This period also sees the increasing inclusion of major US Defense prime contractors.

3. Information Security (2004-2010)

The inclusion of Information Security as a real concern is introduced in 2004 [15], in a case that is non-transactional and derives from Information Security issues. In this case access to information was based on job responsibilities rather than the requirements of the law, which specifies key attributes including nationality. This period also includes cases where access had been granted accidentally due to the capability of IT and the installation of global networks with inadequate access controls. This period continues to include major US Defense prime contractors.

4. Integrated Information Control Systems (2011-2021)

The cases from 2011 onwards see increasing demand for sophisticated IT automation systems that should be applied in a comprehensive and reasonably uniform way across often-global businesses. This period includes several non-US prime Defence contractors. It is not that hardware risks have decreased, indeed several key cases had hardware at their core, rather, the expectation additionally demands a comprehensive Automated Export Compliance system.

To further illustrate this increasing importance of information as both a risk and opportunity, it is worth noting that since the start of Period 2 (Figure 6) when information was first explicitly referenced, the authors have calculated that it featured in over 66% of cases' Proposed Charging Letters (PCLs). Of these cases, over 75% demanded via the Consent Agreement (CA), investment in IT Automation. The above calculations are derived from PCL and CA data sourced from [2].

The level of IT Automation demanded has increased through time, and this is schematically represented in Figure 7.

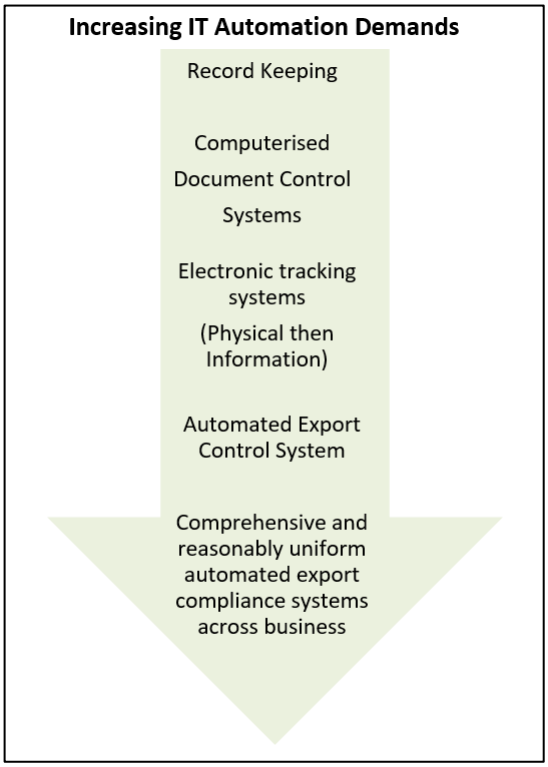

Figure 7: Schematic Representation of Increasing IT Automation Demands (Derived from data in source Ref. [2])

4.3 Results & Discussion 3 – Key Risks Identified

The next area of research was to categorise the key elements of risk arising from the analysis. These are shown in Figure 8. Each of these risks was considered when identifying mitigation IT Technologies (Section 4.5) and process steps (Section 4.6).

Many of these risks are heightened in the information domain compared to the physical one due to the nature of information. For example, securing and quarantining a physical item to prevent unauthorised access by, for example, non-licensed nationals, is an evident and tangible activity – securing information is less so. Whilst a discussion on all the risks is not within the scope of this paper, it is worth highlighting three of the key less obvious ones: -

1. Inadequate and accidental transfers of Export Control information. This risk often materialises when the use of

collaboration technologies are deployed without due consideration to Export Control requirements. At the simple end of the spectrum, technologies such as eMail, web file transfers and file shares are deployed. At the more complex end: collaboration environments, shared data environments and Product Lifecycle Management (PLM) tools may enable unauthorised sharing. Note: More complex products, such as PLMs, often have built-in security models to address the risks.

2. The risk associated with Information Security. This often materialises as a result of the owners of the information not conveying to the providers of the information hosting solution the requirements of the Export Control Licence to be met. Conversely, the Export Control subject matter experts often do not understand enough about the IT environments and the associated security provisions.

3. This risk of a non-transactional Export Control breach. As referenced in Figure 6, this can occur by someone who does not meet the licence conditions simply opening up a document – i.e. no physical export needs to have occurred.

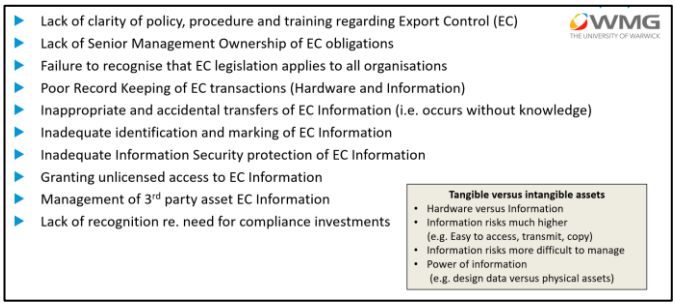

Figure 8 Key Risks Identified in the Analysis (Derived from source (Ref. [2])

4.4 Results & Discussion 4 – Simple Model, Why Complex?

The next part of the research starts to examine why what appears to be a simple process is, in fact, quite complex.

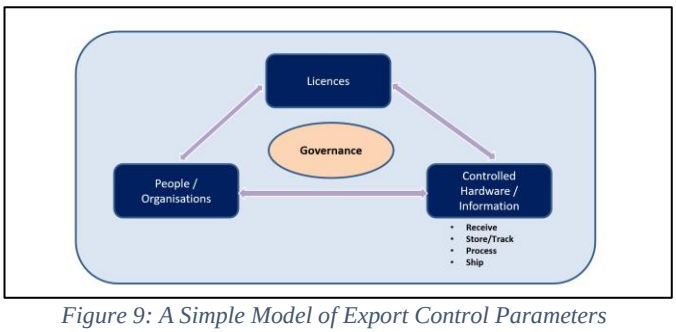

Figure 9: A Simple Model of Export Control Parameters

Consider the diagram in Figure 9. The Export Control parameters may be summarised as: Licences (for the Export Controlled items), People within Organisations, and the Export Controlled items themselves, both hardware and information. At an overview level, the only actions performed on the Export Controlled items are: they are received, processed to add value, stored, and shipped. Record keeping and governance needs to be applied, as represented at the centre of this extremely simplified model. The Export Control system is therefore concerned with managing the interaction between these parameters.

The research being undertaken started to investigate the question 'What then leads to the complexity of Export Control and the materialisation of the risks?'. These risks are as outlined in Section 4.3. Figure 10 depicts that, along with the intrinsic risks in the nature of protecting information, as referred to in Section 4.3, much of the risk is associated with the complexity arising from the variety and volume of these parameters. Further work is to be published in this area, but by way of illustration, recent work undertaken by the authors propose that over 50 attributes regarding a person would be needed to enable access to be granted / denied to all licences under control in an example multi-national company.

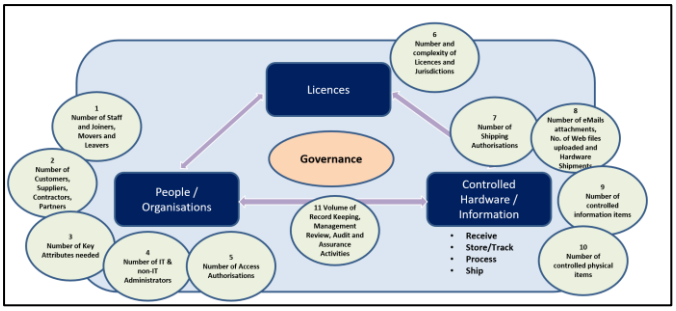

Figure 10: Examples of Complexity Arising From Variety and Volume

4.5 Results & Discussion 5– Risk Mitigation Key IT Technologies Identified

In addition to information risks in Export Control, the use of IT Automation tools offers significant mitigations. These tools as noted in Figure 6 are, in recent cases, demanded by Consent Agreements. These mitigation technologies may apply to physical hardware assets and / or information assets.

Work was undertaken to identify IT Automation risk mitigation technologies, and these are illustrated in Figure 11. Whilst the use of some of these technologies, such as Enterprise Resource Planning (ERP) systems as part of Automated Export Compliance systems are mature, others have less information, particularly on *how* they may be applied.

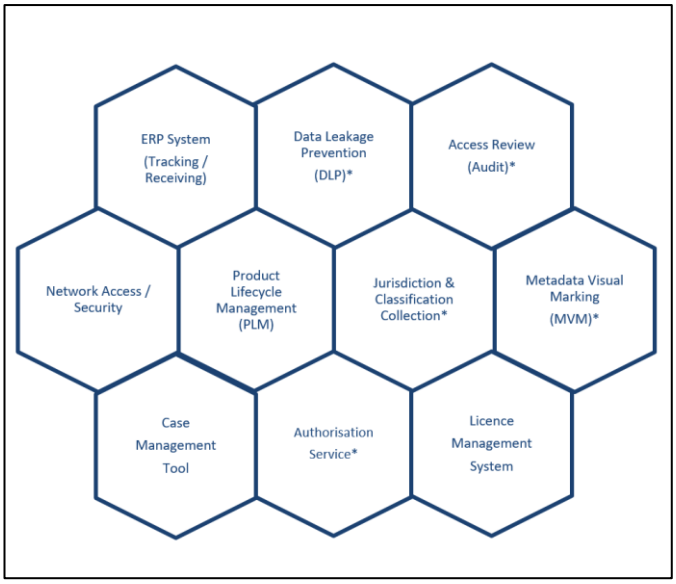

Figure 11: Risk Mitigation - Key Technologies Identified

An example of this is an eMail boundary control, a type of Data Leakage Prevention technology, which, whilst mature, has little documentation on the challenges associated with its deployment. For this technology a paper [16] has been produced by the authors addressing this need. For the examples referenced by * in Figure 11 it is intended that this research publishes further such papers.

An Automated Export Compliance system is a 'system of systems' constructed utilising these types of identified technologies. No two organisations are likely to create the same solution due to existing investments and differing demands.

4.6 Results & Discussion 6– Risk Mitigation Process Steps

Finally, whilst this is in the early stages of its development, this research work establishes the generic steps that organisations can take to address Export Control risks. These steps are represented in Figure 12.

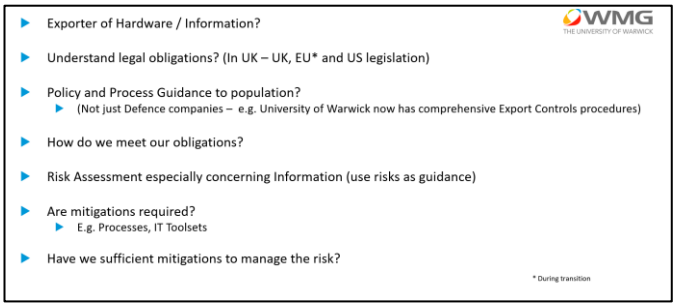

Figure 12: Generic Process Steps for Risk Mitigation

Building upon this work and recognising the importance of Export Control, the University of Warwick has significantly invested in the production of extensive communications and guidance material that now features prominently on the University's Research & Impact Services web pages. The top-level website at the time of writing (October 2021), is as illustrated in Figure 13.

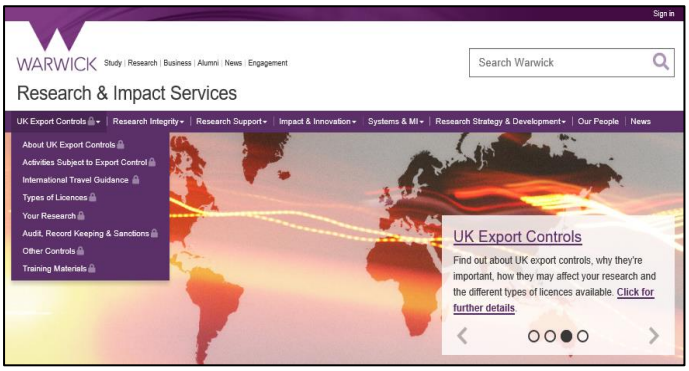

Figure 13: Extensive Export Control Guidance Available at Warwick University (Source Ref. [17])

Additionally, the embodiment of these processes into existing and proposed research work is now complete.

Future work in this area of risk mitigation, including process steps and IT Automation technology case studies (referenced in Section 4.5) should form useful collateral for exporting organisations.

Finally, in addition to the material already discussed, a wealth of information exists for UK exporters on the HM Government websites [18] and [19].

5. Limitations

One limitation of this work is that the Literature Review focuses on US Consent Agreements. Therefore, other risks arising from different regimes' Export Control legislation may exist. Although there are differences, such as the extra-territorial nature of US legislation, many similar characteristics exist. An example of this is the way in which the UK controls the military and dual-use goods through the use of a consolidated controlled list [20]. Excellent guidance exists on UK Export Controls and may be found in the material published [18] by the Export Control Joint Unit (ECJU) and the Department for International Trade. This also includes step-by-step guidance [19] to the export process. This guidance applies to small and large organisations alike, and to Defence and non-Defence organisations.

This work identifies key Information Technologies that can be used to mitigate Export Control risks. Another limitation is that whilst some of the technologies (e.g. ERP) are very well documented in their application, others are less mature and have limited case study material available on the way they are applied. Further work is planned in these areas, an early example being the previously referenced paper [16].

Finally, the generic process steps for risk mitigation are at an early stage in development and, again, more work is planned in this area.

6. Conclusions

The focus of Export Control and Export Control risks has moved significantly from hardware to information. Ensuring that hardware is appropriately controlled remains important, however, the nature of information and the power that can be derived from information makes information a more prominent risk. There is evidence that despite good material being available, organisations do not have appropriate Export Control policy and guidance that is flowed out to their stakeholders.

Information Technology, in addition to being a risk, also offers a wide range of tools to mitigate risks. Several of these tools are well understood and mature, whilst others lack material showing *how* these tools may be applied.

Finally, further research is planned to refine the generic risk mitigation steps and to document case studies of less mature IT Automation tools to aid their more widespread adoption.

7. References

[1] BAE Systems plc, "How to build a Typhoon - workshare," [Online]. Available: https://www.baesystems.com/sites/Satellite?c=BAEMedia_C&childpagename=UK%2FBAELayout&cid=1434554727458&d=Touch&pagename=UKWrapper. [Accessed 26 10 2021].

[2] US - Department of State - Directorate of Defense Controls (US DoS- DDTC), "Penalties and Oversight Agreements," [Online]. Available: https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=384b968adb3cd30044f9ff621f961941. [Accessed 28 07 2020].

[3] US Department of State - Directorate of Defense Trade Controls, "DDTC Compliance Actions," [Online]. Available: https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=e1999c7fdb78d300d0a370131f96193d. [Accessed 26 10 2021].

[4] National Archives and Records Administration's Office of the Federal Register (OFR) and the Government Publishing Office., "Electronic Code of Federal Regulations - The US Munitions List (USML)," [Online]. Available: https://www.ecfr.gov/cgi-bin/text-idx?SID=48ef1ea41aa687906eb5a69f843d39c1&mc=true&node=pt22.1.121&rgn=div5#_top. [Accessed 28 07 2020].

[5] US Department of Commerce - Bureau of Industry and Security, "Commerce Control List (CCL)," [Online]. Available: https://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification/commerce-control-list-ccl/17-regulations/139-commerce-control-list-ccl. [Accessed 27 10 2021].

[6] DDTC - US DoS, "US DoS, Directorate of Defense Trade Controls - Getting and Staying in Compliance with the ITAR downloadable PDF - Compliance Resource," 14 December 2016. [Online]. Available: https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=4f06583fdb78d300d0a370131f961913. [Accessed 09 July 2021].

[7] US Department of Commerce - Bureau of Industry and Security, [Online]. Available: https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear. [Accessed 29 10 2021].

[8] J. McHale, "ITAR compliance: ignorance is no excuse," Military & Aerospace Electronics, 01 07 2009. [Online]. Available: https://www.militaryaerospace.com/computers/article/16709550/itar-compliance-ignorance-is-no-excuse. [Accessed 28 11 2019].

[9] Fried, Frank, Harris, Shriver & Jacobson LLP. Editor: Michael T. Gershberg , "Fried Frank - ITAR Enforcement Digest," March 2020. [Online]. Available: https://www.friedfrank.com/siteFiles/Publications/_ITAR%20Enforcement%20Digest%20on%20US%20Defense%20Trade%20Enforcement_Gershberg_2020%20update.pdf. [Accessed 5 05 2021].

[10] Reuters - Susan Heavey reporting, "Technology: U.S>, Keysight Technologies settle alleged export violations - State Dept," [Online]. Available: https://www.reuters.com/technology/us-keysight-technologies-settle-alleged-export-violations-state-dept-2021-08-09/. [Accessed 28 10 2021].

[11] US - Department of State, "Consent Agreement - Honeywell International Inc.," 27 April 2021. [Online]. Available: https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=e83eab0b1bb764902dc36311f54bcb3b. [Accessed 5 05 2021].

[12] US - Department of State, "Proposed Charging Letter (PCL) - The Boeing Company," 02 09 1998. [Online]. Available: https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=f96db205db15df00d0a370131f96197d. [Accessed 29 07 2020].

[13] US - Department of State, "Proposed Charging Letter (PCL) - Lockheed Martin Corporation," 4 04 2000. [Online]. Available: https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=46ed7a89db99db0044f9ff621f9619fb. [Accessed 25 09 2020].

[14] US - Department of State, "Proposed Charging Letter (PCL) - Raytheon Company," 2003. [Online]. Available: https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=b21e7e89db99db0044f9ff621f961937. [Accessed 28 10 2021].

[15] US - Department of State, "Draft Charging Letter (DCL) - General Motors Corporation & General Dynamics Corporation," 2004. [Online]. Available: https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=4d8df205db15df00d0a370131f96196b. [Accessed 25 09 2020].

[16] J. G. Dunn, C. Maple and G. Epiphaniou, "Management Challenges in the Implementation of an email Boundary Control for Data Leakage Prevention," in *Competitive Advantage in the Digital Economy (CADE) 7th CADE Conference*, Online (Virtual Venice), 2021.

[17] University of Warwick, "Research & Impact Services," [Online]. Available: https://warwick.ac.uk/services/ris. [Accessed 28 10 2021].

[18] HM Government UK, "Guidance - Exporting Controlled Goods," 21 December 2020. [Online]. Available: https://www.gov.uk/guidance/exporting-controlled-goods-after-eu-exit. [Accessed 23 07 2021].

[19] HM Government UK, "Guidance - Exporting Controlled Goods," 21 12 2020. [Online]. Available: https://www.gov.uk/export-goods. [Accessed 28 10 2021].

[20] HM Government UK - Departent for International Trade, "UK Strategic Export Control Lists," 01 2021. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948279/uk-strategic-export-control-list.pdf. [Accessed 29 10 2021].