HEECA The Higher Education Export Control Association

Export Due Diligence Process Guidance

Acronym Cheat Sheet:

BSR	Basic Scientific Research
ELA	Export Licence Application
NLR	No Licence Required
OGEL	Open General Export Licence
OITAL	Open Individual Technical Assistance Licence
SIEL	Standard Individual Export Licence
WMD	Weapon of Mass Destruction

Introduction

This guidance describes the main structure of an export due diligence process in relation to end-use controls. It does not describe how to undertake a technical assessment against the UK Consolidated Strategic Export Control List – each UK Higher Education Institution (HEI) should support their researchers in doing this assessment separately.

How do the "Basic Scientific Research" and "In the Public Domain" exemptions relate to the export due diligence checks institutions should undertake, as part of their risk management portfolio?

Independent of a UK HEI's risk appetite, all institutions should start the process of risk management assessing the project's related technology, software and physical goods against the UK Consolidated Strategic Export Control List to determine if any of them fall under any of the controlled entry codes, or if it could fall under either of the 'Basic Scientific Research (BSR)' or 'In the Public Domain' exemptions.

The second part of this risk management process should include due diligence checks that consider the end-user controls (see figure 1).

It is during **Part I** of the self-assessment (usually undertaken by the researchers) that the consideration of the exemptions of 'In the Public Domain' and 'BSR' arise.

Part II of the end-user controls is advised to be undertaken by a Central University Team (that is, a second pair of eyes, independent from the researchers involved in the project).

Note: if a project has been self-assessed as controlled technology as per the UK Consolidated Export Control List (i.e. applied technology meeting the technical thresholds described in the consolidated list), it will never be "decontrolled" by the BSR exemption. There are notes included in the UK Consolidated Export Control List that can 'decontrol' items or technology based on their characteristics or thresholds.

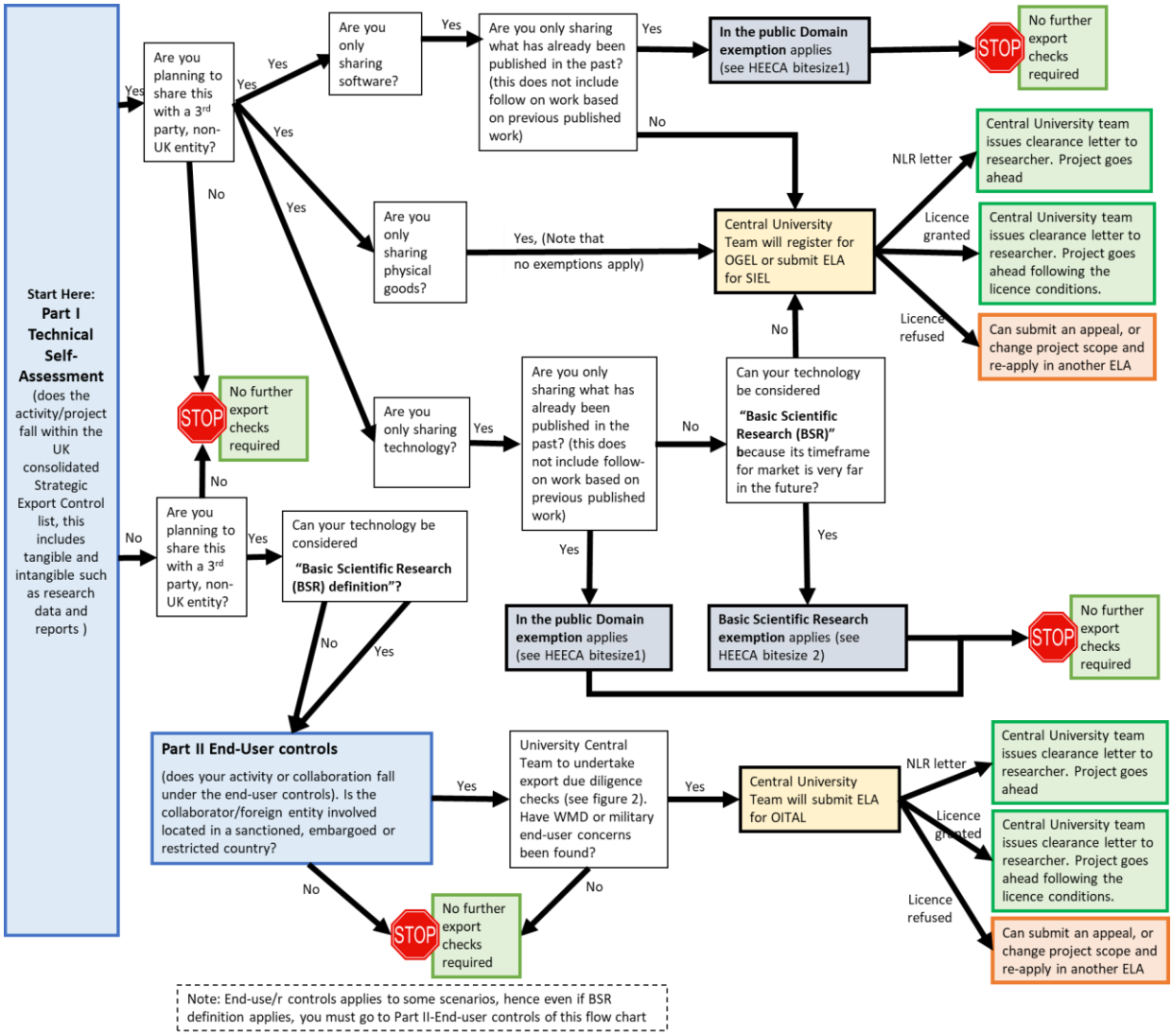

Figure 1. Flow chart depicting the relationship between the exemptions of 'In the Public Domain' and 'BSR', and End-user controls in the requirement for export due diligence checks.

Main structure of an export due diligence process considering end-user controls

Any export due diligence process or programme should have three parts:

Part I: Scoping, what academic activities and what projects fall within the scope of export controls. This step should identify that most academic projects will fall outside of the scope, hence not requiring to undergo export due diligence checks. Different institutions with different risk appetites will define what falls within the scope of their export due diligence programmes (see **Table 1** for suggested points to consider).

Part II: Basic checks, around the nature and activities of the foreign entity (intrinsic entity checks) and checks related to the project at hand with that entity. Note that most of the activities/projects that trigger export due diligence, will require just these basic checks, where each institution should be able to clear them internally, without the need of reaching to government for advice (est. 90% of all queries to be cleared in house – see **Table 2** for suggested points to consider).

Part III: Advanced checks, which involved utilising open-source information, and commercial packages to gather more intelligence on the foreign entity and identification of any links to the military. This enhanced due diligence stage also includes advice from various government departments; from RCAT, as informal consultation on concerns on the project and foreign entity where needed; and from ECJU, in the shape of End-User Advice (EUA service) required for formal advice on WMD and/or military concerns on the foreign entity, as well as through Export Licence Applications (ELA) for formal approval of that particular project to that particular end-user. Note that only a few (est. 10% of queries) require an ELA. Informal consultation with RCAT, where needed, should decrease this number further (see **Table 3** for suggested points to consider).

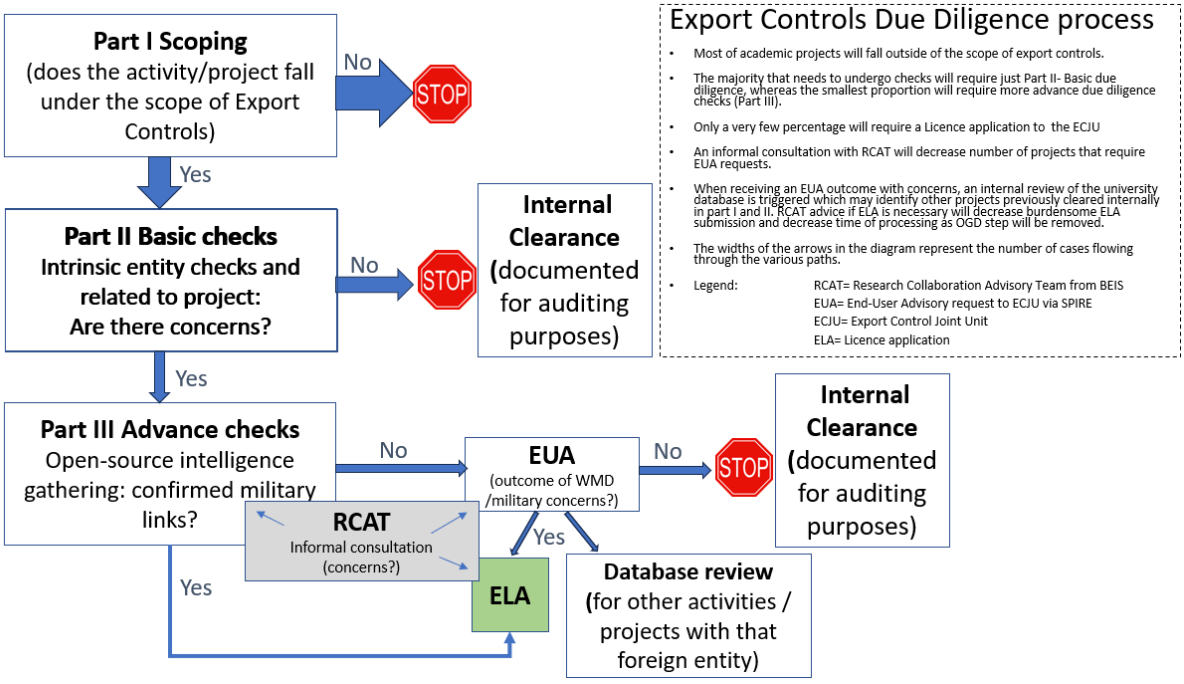

Figure 2. Diagram depicting the structure of an export due diligence process / programme consisting of three main parts: Scoping, Basic checks and Advanced checks.

Note: the widths of the arrows represent the number of cases flowing through the various paths, to flag how only a few percentages go through the whole process of requiring a submission to ECJU in the form of an ELA.

Part I: Scoping

Each institution will establish which activities will trigger the requirement of export due diligence checks under end-user controls based on their risk appetite, and on the advice received from RCAT, where requested. Remember that if something has already been self-assessed as controlled as per UK Consolidated Export Control List, it will need a licence in place to enable that export or transfer across UK borders. No further export due diligence under end-user controls is required as the assessment of the ELA by the team in ECJU will look into that aspect during the processing of the ELA.

Table 1 contains some points to consider when deciding what should be inside or outside of the scope of export due diligence related to end-user controls.

Inside of scope of Export controls	**Outside of scope of Export controls**
Related to the 10 categories of the UK Consolidated List <u>but not meeting thresholds</u> to be considered controlled, i.e. it does not fall under a specific entry code.	Is the project related to undergraduate teaching without final year placement/research projects?
Other areas: - Advanced Materials - Artificial Intelligence - Data Infrastructure - Cryptographic Authentication - Biotechnology - Fermentation - Synthetic Biology - Chemistry and chemical engineering - Physics - Instrumentation and sensors - Satellite and Space Technologies - Civil Nuclear - Defence - Energy - Transport - Suppliers to the Emergency Services - Computing Hardware - Quantum - Biochemistry - Genomics and other "omics" involving human cells - Production and process technology - Electrical engineering - Mechanical engineering Robotics - Nuclear waste and water/soil research - Critical Suppliers to Government - Telecommunications and information technology	Research or teaching areas outside the areas on the left column: Languages, Nursing, Anthropology, Economics, Finance
	Donors to University without links to specific research
	PGR and PGT students who don't have any other external affiliation (e.g. they are 100% students of your institution, not split site students)
	High level discussions among researchers
	Conference attendance
	Third-party student recruitment agencies

• Research collaborations • Funders of research projects • Short- and long-term visiting researchers in campus • Remote access by "remote" visiting researchers • Integrating industrial partners as placements for master students • Partial appointments overseas	Signature of Memorandum of Understanding or Head of Terms, which do not have any special confidentiality clauses (Any project/activity as visitors under this MoUs should undergo due diligence when it takes place)

Part II: Basic checks

Each institution will decide if they will use a third-party company to undertake their due diligence checks or if they will do it internally. Basic checks should cover both looking at the intrinsic nature of the entity **and** the risk associated with doing that specific project with that particular entity, i.e. a conjoined risk.

Table 2 contains some points to consider when undertaking these basic checks as part of the export due diligence related to end-user controls.

Intrinsic Entity checks	Checks related to the collaboration project
Is it listed as Medium, High or Very High Risk in the Australian Strategic Policy Institute (ASPI) Tracker? Note: Depending on the risk appetite of your institution you may want to proceed with only the Very High or with all except the Very Low, at both ends of the spectrum of risk appetite.	Is the project on a subject that is not of concern but the entity is working on an area of concern? Why are they interested in this project? (e.g. missile manufacturer collaborating on biological drug testing in model organisms)
Is this entity listed in a published governmental list such as UK Sanctions List, U.S., EU or UN? Note: you may want to utilise a commercial software to answer this question at the push of a button.	If the entity is not working on an area of concern but they do not work on the area of the project either, why are they interested in this project? Is there a possibility of diversion?
Does your institution have previous knowledge of WMD /military concerns on this entity?	Request for upmost confidentiality with respect to the details of the content of services and the contract

Note: EUA outcomes have a validity of 6 months (NLRs) and 12 months for concerns	
Is there concealment of the end user by the use of harmless-sounding company names or the use of state universities as alleged end users?	Are there unusually favourable terms of payment? (e.g. excessive fee or advance payment in cash)
Is the entity from the military sector? (e.g. those acting on behalf of a ministry of defence or the armed forces) Are there known business contacts of the entity with the arms industry or nuclear facilities?	Are they using a neutral or misleading project title for what the nature of the project is in reality? Explanations by prospective (cooperation) partners give the impression that the projects refer to basic scientific research although this is not the case.
Does it have a reliable website?	Has there been a transfer of a foreign scientist (student, doctoral student etc.) to the research project without his/her previous activity having any connection with it?

Part III: Advanced checks

This final enhanced due diligence includes researching open source for further intelligence on military links to the entity as well as contacting the UK Government for advice (RCAT and ECJU).

It is advisable to contact RCAT at this stage of the due diligence process to determine the level of risk associated with the technology/partner and whether the legislation could apply. There is no obligation engaging with RCAT for advice, however, your institution can request their advice for any individual cases that are needed. You can informally discuss any concerns you have about a specific project with a specific entity before submitting ELAs to ECJU. This informal consultation will decrease the number of projects that may require EUA requests as well, reducing the burdensome ELA submission and decrease the time of processing for ECJU.

When receiving an EUA outcome from ECJU, an internal review at the UK HEI should be triggered which may identify other projects previously cleared internally in **Part I** and **Part II** of the export due diligence process. Based on the risk appetite of your institution and research security knowledge, your institution may informally consult RCAT if further ELAs are necessary for any of the ongoing projects identified in the review.

Table 3 contains some points to consider when undertaking the enhanced due diligence Part III of the export due diligence related to end-user controls.

Part III Advanced checks - Points to consider
To reduce the time of processing, once you have internally identified military links, go directly to ELA instead of using the EUA service as an intermediate step.
If RCAT advice (where sought) has determined that legislative measures could apply to the activity, it is advised to use the End-User Advisory (EUA) request service in the portal, SPIRE (soon LITE) to confirm if ECJU has concerns of WMD or military on that particular entity.
If the EUA outcome is of WMD or military concerns, this doesn't mean that you cannot engage in the research collaboration. You just need to submit an ELA to ECJU. This licence would be for transfer of technology (not coded) and the technical assistance under the end-user controls (see SOP on the **HEECA Resources** webpage on how to prepare these ELAs).
When receiving an EUA outcome with concerns (WMD and/or military), an internal review of the university database should be triggered which may identify other projects previously cleared internally in **Part I** and **Part II** involving that entity of concerns.

Additional links:

GOV.UK - Export Control Exemptions
GOV.UK - Export Controls on Academic Research (Case Studies)
GOV.UK - Export Controls Applying to Academic Research (Guidance)
GOV.UK - End-use Controls Applying to WMD-related Items (Guidance)
GOV.UK – Recognising suspicious enquiries
HEECA Guidance: 'In the Public Domain' Exemption