



DEFENCE EXPORT CONTROLS **AUDIT FACTSHEET**

There are two types of audit that can occur, depending on the circumstances

1 Entity Self-Audit

An entity self-audit can be completed by the permit holder to ensure organisations comply with Defence Trade Controls Act 2012. Should an issue arise (such as a potential breach of legislation) best practice is to notify DEC Compliance as soon as possible with mitigating circumstances to assist in the support provided.

2 Desktop Audit

A Desktop Audit is conducted by Defence Export Controls (DEC) to check historical exports and the permit's amendments, details and compliance history to determine potential breaches or further reporting is required.



SELF-AUDIT PRINCIPLES

Defence Export Controls offers easy-to-follow guidance to help organisations conduct voluntary internal self-audits.

Regular self-audits involve regulated entities reviewing their internal documentation to confirm they meet record-keeping and permit requirements which you can provide to Defence.

Self-audits are voluntary and cannot be enforced by Defence Export Controls.

Self-Audit Steps

- ➔ **Access templates:** Use the Self Audit Checklist available through the My Australian Defence Exports (MADE) portal.
- ➔ **Conduct the Self-Audit:** Review all relevant information from Defence Export Controls, including compliance resources, and review internal records.
- ➔ **Notify DEC:** If a potential breach is identified, notify DEC through the MADE portal using the Voluntary Disclosure template.

Consequences of Non-Compliance

- ❗ Non-compliance can result in criminal charges. If found guilty of an offence, penalties of imprisonment and/or fines can be imposed.
- ❗ Publicity resulting from non-compliance can lead to significant reputational damage.
- ❗ Regulatory investigations and sanctions can disrupt business operations.

Red Flag Indicators

What to look for in controlled activities

- Freight Forwarders as Final Destination:** Used to hide the true recipient or purpose.
- Refusal to Disclose End-Use:** Could indicate potential misuse or diversion.

Business Mismatch:

Suggests the buyer may not be the actual end-user.

Suspicious Shipping Routes:

May signal efforts to bypass export controls.

Unusual Payment Methods:

Can indicate attempts to avoid transaction records.

Contact us

- 🌐 defence.gov.au/business-industry/export-controls
- ✉ exportcontrols@defence.gov.au
- ☎ 1800 DEFENCE, Option 4

