AI Chip Export Compliance Checklist

Securing the Supply Chain Against Diversion and Remote Access Risks

Recent investigations highlight that paper-based compliance is no longer sufficient. Cloud access, third-country data centres, and staged audits are emerging vulnerabilities. Use this checklist to review your exposure to US (EAR), UK, and EU dual-use controls for advanced AI chips.

1. Enhanced Due Diligence & Screening

Re-screen high-risk regional hubs: Conduct enhanced due diligence on all resellers, distributors, and data centre clients in Southeast Asia (e.g., Singapore, Malaysia, Indonesia, Thailand).

Verify compute location: Ensure you are verifying where the computing power is actually utilized, rather than merely checking the physical hardware delivery address.

Review US re-export exposure: If operating outside the US (e.g., UK or EU), map your supply chain to confirm adherence to US extraterritorial rules for US-origin items.

2. Physical & Technical Verification

Conduct physical site visits: Back up End-Use Certificates (EUCs) with physical inspections to verify that environments are active production sites, not staged "dummy" server rooms.

Perform serial-number reconciliation: Mandate routine checks to ensure deployed chips match licensed exports exactly.

Map cloud access architecture: Audit remote-access pathways and IaaS offerings to identify where restricted parties could potentially access controlled computing power remotely.

3. Audit Integrity & Insider Threat Protocols

Secure the audit process: Treat external auditors and internal due-diligence staff as potential targets for espionage or inducement.

Update compliance policies: Explicitly bring rules regarding hospitality, conflicts of interest, and bribery into the core export compliance program.

Implement frontline training: Train sales, logistics, and technical teams to identify red flags, inducement risks, and appropriate escalation paths.

4. Regulatory Horizon Scanning

Monitor BIS remote-access guidance: Track updates from the Bureau of Industry and Security regarding cloud computing and remote hardware access.

Track legislative developments: Stay informed on the progress of the Chip Security Act (requiring location tracking of exported chips) and the AI Overwatch Act.

Need to assess your exposure?

Export compliance is no longer just a licensing exercise. **clearBorder** supports manufacturers, distributors, data centre operators, and investors with expert risk assessments, site verifications, and compliance program design.