Export Controls
An increasing challenge to comply
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:30 – 14:00</td>
<td>Welcome &amp; registration</td>
<td></td>
</tr>
<tr>
<td>14:00 – 14:30</td>
<td>Update &amp; Recent evolutions</td>
<td>Giovanni Gijsels</td>
</tr>
<tr>
<td>14:30 – 15:00</td>
<td>Export Control Compliance Framework</td>
<td>Laurent Claassen</td>
</tr>
<tr>
<td>15:00 – 15:30</td>
<td>Restricted Party Screening: Industry practices</td>
<td>Nick Moris</td>
</tr>
<tr>
<td>15:30 – 15:45</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>15:45 – 16:15</td>
<td>Data as a controlled element</td>
<td>Luc Beirens</td>
</tr>
<tr>
<td>16:15 – 16:45</td>
<td>Export Control Sanctions</td>
<td>Alexander Baert</td>
</tr>
<tr>
<td>16:45 – 17:00</td>
<td>Wrap up and closing remarks</td>
<td></td>
</tr>
<tr>
<td>17:00 – …</td>
<td>Reception</td>
<td></td>
</tr>
</tbody>
</table>
Export Controls
Update & Recent evolutions

Giovanni Gijsels
28 April 2015
Recent events
The Dark side

Cyberattack on U.S. Infrastructure
A highly disruptive cyberattack on U.S. critical infrastructure

Pentagon to Unveil Cybersecurity Strategy
U.S. Defense Secretary Ashton Carter is expected to unveil the Pentagon’s cybersecurity strategy in a speech at Stanford University on Thursday. The strategy, which stresses deterrence and transparency, will include plans to set up a permanent outpost in Silicon Valley and forge ties with the private sector. (updated April 23, 2015)
Recent events

The silver lining

President Obama Delivered a Statement on Cuba

We are separated by 90 miles of water, but are brought together through shared relationships and the desire to promote a democratic, prosperous, and stable Cuba. President Obama is taking action to cut loose the anchor of failed policies of the past, and to chart a new course in U.S. relations with Cuba that will engage and empower the Cuban people.
Export Controls
A short recap
Export Controls
What are they?

EU Commission:

“Export controls, as a security-related trade instrument, remain, more than ever, at the forefront of international non-proliferation efforts. They need to adjust to the evolution of security risks and threats – including the various forms of terrorism and the efforts by some States and non-state actors to acquire weapons of mass destruction and corresponding carrier technology and armaments”

These controls are closely linked with the restrictive measures that exist (e.g. Russian sanctions):

“In general terms, the EU imposes its restrictive measures to bring about a change in policy or activity by the target country, part of a country, government, entities or individuals. They are a preventive, non-punitive, instrument which should allow the EU to respond swiftly to political challenges and developments.”
Export Controls
The four cornerstones

Product Controls
- Military or weapons
- Dual use
- Other definition
- Other
- Includes technology and intangibles

End User
- Who will be the recipient of the product?
- Including all entities involved in a transaction

END USE
- What is the product used for?
- “Catch-all” provision

SANCTIONS
- Where is the product going to?
- What can be shipped to that destination?
The interactions of the “four cornerstones” can lead to a situation in which:

- Transactions are “business as usual”
- Transactions are allowed, but require careful consideration
- Transactions can be allowed after government approval
- Transactions cannot proceed
Export Controls
Updates
The new European Dual-Use List is set out in Annex I to the regulation and replaces the existing Annex I of Council Regulation (EC) No 428/2009 as of 31 December 2014

Concretely:

• Based on changes on a **global** scale (e.g. US reform)
• **400 revisions** cover 10 dual use categories, mainly to the notes
• **Addition and/or specification** of various dual use items were foreseen such as *graphite*, *frequency changers*, *machine tools*, *viruses/toxins*, *integrated circuits and explosives*
• Changes based on **recent experience**: IT intrusion software ('spyware'); telecom & “internet surveillance” equipment
• Removal of **low risk** or very common products

• “…to fully comply with its **international security obligations** and maintain **exporter competitiveness**…”
Product controls

US reform

In 2009 the Export Control Reform Initiative was announced by President Obama to:

- Change from a system that meets the challenges of the **Cold War world** to one that meets the challenges of the **21st Century**
- Reduce the **harmful effects** of the current control lists on US manufacturers
- **Enhance, not ease**, the prohibitions (T5 countries, China’s military modernization program – 0% de-minimis rule)
- Create a “**bright line**” between the **U.S. Munitions List and Commerce Control List** (e.g. shift from military to EAR “600 series”)
- Build towards a **single control list**, single **licensing agency**, unified information technology system, and **enforcement coordination center**
Products and & End Use

Chemical exports

Companies should always be aware when:

- Activities are done in **sensitive** regions
- Products could be “**misused**” (even though they might not be controlled)
- Transactions contain any **red flags** (unclear parties, suspicious quantities,…)

Following a chemical attack in Syria, a number of European Companies got bad publicity although the transactions were allowed at the time
Japan recently updated its End User List (15 April 2015):

- **527 entities in 11 countries** and regions are covered
- Entities for which concern cannot be eliminated that there is **involvement** in the development of WMD
- This is **no embargo**, but can trigger license requirements
- This entails a **combination** of End User, End Use and Product controls
Sanctions
Wide impact of Russian restrictions

Embragos and sanctions can be imposed by the UN, the EU, national and even regional authorities. The impact could be wider than typically for dual use (extraterritorial application).

Example for Russia:
- In force as of **1 August 2014**
- 3 **export** restrictions, 1 **capital** market restriction
- Concerns **more than goods**:
  - Direct or indirect technical assistance
  - Financing or financial assistance
  - Brokering services

**Dual-use goods** intended for military end-users
**Energy-related equipment** subject to license, not for oil projects
**Military items** for both import and exports
**Capital markets** for state-owned Russian banks and filiation
“if there’s any way they can do it wrong, they will”
Edward A. Murphy (1918–1990)

“If you think compliance is expensive, try noncompliance.”
Former U.S. Deputy Attorney General Paul McNulty
Export Controls: Update & recent evolutions

Questions

Giovanni Gijsels
Senior Manager
Customs & Global Trade
gijsels@deloitte.com
+32 477 565 949
From firefighting to management by exception

- Remedial & corrective actions
  - Record keeping & Controls
  - Internal audit & Monitoring
  - Risk & Trade analysis
  - Screening
  - Reporting
  - Organization & commitment
  - Policies & Procedures
  - Training & Awareness

- Firefighting
- Ad-hoc investigations and research
- No corporate awareness

- Constant issue solving
- Exception management
- Management by exception
  - Day-to-day activities supported by automation
  - Foundation of Compliance

© 2015 Deloitte Academy
Deloitte’s approach for an Export Control Compliance Framework

Five distinct elements

Deloitte has indicated the need for several work packages in order to be on top of Export Control Compliance. A comprehensive framework should at least contain these five elements.

Deloitte can provide with single modular services or help setting up a complete Export Control Compliance Framework with various tooling options.

Our modular services include:

- Export Control Risk Assessment: identify key risks by risk assessments or reviews
- Policy and Procedures: evaluate, set-up and roll out of export policy and procedures (including training and awareness)
- Export Control Organization: Compliance program development, organizational design, Export Compliance function, roles & responsibilities
- Export Control Classification: classification of products and licensing management, supported by automation
- Sanction and Embargo Screening: trade automation and management solutions, in line with the company’s policy and embedded within the organization
**Work Packages: Identify key risks in Export Compliance**

**Objectives**

- Develop a guideline for the risk assessment based on the legal requirements (e.g. definition on roles and responsibilities within the organization)
- Develop a standardized questionnaire and reporting tool
- Develop the process of the risk assessment (e.g. top down approach with workshops, bottom up approach through analysis of processes, functions and export control organization)
- Establishing priorities for the rollout of the risk assessment

**Approach**

- Define a risk framework (based on ERM applied by the company) and the scope
  - Risk sessions:
    - Develop long list of risks based on interviews, analysis of existing materials
    - Assess risks during risk assessment sessions
  - Assess the identified risks during risk assessment sessions, making use of anonymous voting technology
  - Report on risk priorities with heat map and define recommendations

**Deliverables**

- Validated questionnaire
- Definition of risk template
- Risk assessment (interview sessions and assessment sessions)
- Risk heat map
- Recommendations for risk mitigation
- Concept risk template and approach

---

**Preparations and scoping**

- Examine current ERM
- Business: define the scope
- Define risk template & questionnaire

Preparations in close collaboration with the company

**Risk assessment**

- Risk assessment
  - Interviews
  - Assessment

**Reporting**

- Risk assessment
  - Risk heat map
  - Recommendations
Deloitte performed various type of risk assessment for large international corporations. Deloitte has developed a proven methodology which can be used in a wide variety of risk assessments.

Deloitte methodology for risk assessments

**Phase 1: Requirements**
- Regulatory obligations are mapped on key export compliance themes (EU export regulation, US export regulation (EAR & ITAR), (international) sanctions (e.g. EU, US, UN) and Compliance Framework) taking business strategy and core values of the organization into consideration

**Phase 2: Intelligent scoping**
- Key Risk Indicators for the in scope theme and assessment unit types (organization unit, process, product) are determined.
- Business Units with similar risk profiles, control environment and jurisdiction are combined into Assessment Units.
- Prioritise efforts and focus on high risk areas. Create a basis for efficient group wide risk assessments.

**Phase 3: Risk Identification and assessment**
- By using best practice, risk & control databases and strong facilitation techniques, risk profiles per Assessment Unit are determined.
- Identified risks are assessed based on impact and likelihood scales which are aligned to the organization’s standards and definitions using our best practice risk assessment tools.
- Inherent risk is determined at Assessment Unit level and group level.

**Phase 4: Control identification and gap analysis**
- For all identified and assessed risks the control activities are documented. Granularity of control documentation is based on inherent risk profile. The best practice control activity database is available to challenge local management in identifying the appropriate control.
- Control gaps are identified and risk response (Accept, Reduce, Share, Avoid) is defined.
- Residual risk is determined at Assessment Unit level and aggregated at Group level.

**Phase 5: Control gap remediation**
- For identified control gaps, the business undertakes remedial actions undertaken based on the best practice control activity database.
- Risk & control registers and identified gaps for the Assessment Unit are applied to all organizational units in the Assessment Unit.
- Compliance function advises business regarding risks and controls.

**Phase 6: Monitoring**
- Compliance Monitoring plans are created based on risk profiles, identified control gaps and residual risks.
- Findings are fed into the PDCA cycle to improve the processes and IT.
### Identify key risks in Export Compliance

**Approach risk assessment**

<table>
<thead>
<tr>
<th>Preparations</th>
<th>Actions</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• In co-making with the company we will align our methodology (process, likelihood &amp; impact scales, best practices risk and control registers and assessment tooling) to your internal risk assessment practices</td>
<td>• Proven and customized methodology for Export Compliance Risk Assessments</td>
</tr>
<tr>
<td></td>
<td>• In co-making with the company we develop guidelines for the risk assessment, including definitions of impact &amp; likelihood, documentation standards for risk &amp; controls and align existing Risk Management and Compliance processes</td>
<td>• Able to share a detailed plan of approach, including the level of granularity applied in the assessment</td>
</tr>
<tr>
<td></td>
<td>• Detailed plan of approach, including definition of assessment units, questionnaire and set up of end-to-end process, will be prepared for the company</td>
<td>• Export Compliance Risk Assessment process</td>
</tr>
<tr>
<td></td>
<td>• Proven and customized methodology for Export Compliance Risk Assessments</td>
<td>• Tooling to support the assessment process</td>
</tr>
<tr>
<td>Execute Risk assessment</td>
<td>• Assessments will be conducted in workshops</td>
<td>• Trained and experienced company staff for the future in conducting these assessments using the methodology</td>
</tr>
<tr>
<td></td>
<td>• Training on the job for the company’s facilitators</td>
<td>• Oversight over theme ‘Export Compliance’ at location level as well as for the company’s Operations level</td>
</tr>
<tr>
<td></td>
<td>• Deloitte will prepare risk &amp; control reports on Export Compliance</td>
<td>• Risk assessment report including heat map</td>
</tr>
<tr>
<td>Report findings</td>
<td>• Deloitte will report the results of Risk assessments consolidated.</td>
<td>• A proposal for risk response (follow up)</td>
</tr>
<tr>
<td></td>
<td>• Part of the report is the heat map which includes assessment of the risks in likelihood and impact.</td>
<td>• Roadmap for Export Compliance Framework and implementing controls</td>
</tr>
<tr>
<td></td>
<td>• Propose follow up actions depending on risk appetite to control and mitigate identified risks</td>
<td>• Tested methodology for Export Control risk assessment</td>
</tr>
<tr>
<td></td>
<td>• Roadmap to implement controls</td>
<td>• Assistance in executing Roadmap to implement Export Control Compliance Framework</td>
</tr>
<tr>
<td>Evaluate</td>
<td>• Deloitte and the company will evaluate the risk assessments, including lessons learned</td>
<td>• Deloitte can assist the company in remedial and corrective actions</td>
</tr>
<tr>
<td></td>
<td>• Document methodology for the company</td>
<td></td>
</tr>
<tr>
<td>Follow up actions</td>
<td>• Deloitte can assist the company in remedial and corrective actions</td>
<td></td>
</tr>
</tbody>
</table>
# Identify key risks in Export Compliance

Intelligent scoping

## Company Entity Summary

<table>
<thead>
<tr>
<th>Structure</th>
<th>Assessment Unit</th>
<th>Overall risk indicator</th>
<th>Product risks</th>
<th>Export risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Belgium (HQ)</td>
<td>1</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>UK</td>
<td>1</td>
<td>M</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Switzerland</td>
<td>1</td>
<td>N</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Germany</td>
<td>1</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>

### Risk Factors

**Product risks**

**Classification of products and services**
- Military goods or technology: High
- Dual-use goods or technology: Medium
- Civilian goods or technology: Low

**End-use**
- Military: High
- Dual-use: Medium
- Civilian: Low

**Export risks**

**End-user**
- Sanctioned customers or unknown: Very High
- Military customers: High
- Civilian custumers: Medium
- No customers: Low

**Destinations**
- Sanctioned countries: Very High
- High risk countries (based in transparency International): High
- Within EU: Low

---

### Assumptions

- Our methodology includes a robust scoping mechanism by using 4 indicators for identifying Export Compliance risks, which enables to focus on the activities in areas with the highest risk.
- Rating all locations provides insight in different classes of locations (and subsidiaries).
- Events and audit reports as well as size of the organizational unit might impact risk classification.
- In this scheme Company’ Risk appetite is not taken into consideration.

Please note that this is indicative assessment requiring further risk classification in collaboration with the company. H, M, L indicators are relative scores used to classify and prioritize assessment units and do not reflect inherent risk.
**Work Packages: Set up policy and procedures**

**Objectives**

- Evaluate current structure and methodology of policies and procedures
- Assess current policy and procedures concerning Export Control Compliance
- Develop Export Control policy
- Develop Export Control procedures
- Create an effective roll out of the policy and procedures
- Create the necessary awareness concerning the new policy and procedures

**Approach**

- Desk research (current policy and procedures, legal requirements)
- Interview with experts (policymakers, legal department, subject matter experts)
- Drafting concept policy and procedures and gathering feedback from the company
- Develop a communication approach

**Deliverables**

- Export Control policy
- Export Control procedures (framework)
- Management presentation on new policy and presentation
- Training materials for the company's trainers
- Communication approach for designated employees

**Preparations and scoping**

- Desk research
  - Current policies & procedures and methodology
  - Gather legal requirements

Preparations in close collaboration with the company

**Drafting**

- Input Risk assessment
- Draft EC Policy for the company
- EC procedures manual (Group + location specific)

**Roll out**

- Awareness creation
  - Management presentation
  - Train the trainer
  - Communication approach
Work Packages: EC requires organizational changes

Objectives

- Develop an organization structure that contains the core elements of an effective Export Control Compliance Framework. After execution of the Roadmap for implementation the new EC organization should realise the following objectives:
  - The company is able to detect export compliance risks in an early stage and takes sufficient actions to mitigate identified risks
  - Adequate Export Compliance policy, procedures and controls are in place and effective
  - The company Higher management encourages compliancy (organizational commitment / tone at the top)
  - The company is an organization that protects employees (including temporary staff) through training and awareness programs from (inadvertently) violating Export Controls
  - Business partners (e.g. employees, suppliers, contractors, customers), transactions, staff, visitors and transactions are screened
  - Adequate recordkeeping of export compliance related data (licenses, transactions, business partners etc.) and audit trail
  - Export Control is part of an internal and external audit & monitoring program of the company
  - The company has an internal reporting mechanism and maintains a program for handling compliance incidents, including reporting export violations
  - Develop an organization that provides compliance safeguards throughout the company’s supply chain to ensure consistent export decisions and order processing.

Approach

- Define key risk areas (input from WP 1)
- Analyze current organizational structure
- Draft design Export Compliance framework
- Determine gaps (gap analysis)
- Draft Export Compliance policy & procedures (WP 2)
- Draft functional descriptions and assign roles & responsibilities
- Draft Roadmap for implementation of EC organization

Deliverables

- Design Export Control Compliance Framework
- Overview required governance and functions
- Design Roadmap for implementation

Preparations and scoping

- Input Risk Assessment
- Policy and Procedures
  - Snapshot of current organizational structure

Design

- Draft
  - Functional descriptions
  - Organizational design
  - Roadmap for implementation

Execution

- Assign Roles & Responsibilities + staffing
- Delivering:
  - EC Compliance Framework
  - Overview governance and functions
  - Roadmap
- Execute Roadmap
# Work Packages: Classification of products and data

## Objectives

- Review current classification procedures, perform research on the products and define applicable legislation.
- Identify Export Control Compliancy rate
  - Gain a view of the impact of export control compliance on the product portfolio
- Design a classification methodology (for instance family grouping and designing classification decision trees)
- Assess the possibilities for master data management and automation
- Implement the export control classification procedure in the business processes (e.g. the Product Approval Process)

## Approach

- Perform research on the products and applicable legislation.
- Define family grouping, sample methodology a classification methodology using decision trees
- Map the existing IT landscape in view of product classification and maintenance: check where is data maintained, master data is set up and managed, which systems are being used, what is the level of automation.
- Define requirements for (potential) future system solution(s) for export control classification data and controls

## Deliverables

- Overview of EC Compliancy for the product portfolio
- Classification methodology based on decision trees
- Fit gap analysis for system support
- IT Design and Roadmap with requirements (short list requirements)

### Preparations and scoping

- Desk research
  - Goods, technology and services in scope
  - Gather EU and German legal requirements
  - Current system and data management landscape

### Classification

- Input Risk assessment
- Define classification methodology and draft product classification decision trees (6/8 products)
- Define system support requirements & Fit-Gap analysis
- Input Policy and Procedure

### Roll out and roadmap

- Integrate classification procedure in business processes (e.g. Product Approval)
- IT Design and Roadmap with requirements
- Input Screening (IT)
Tender-request for exporting items, services or data

Determine if the export item is classified in Category 0 (Nuclear Dual-Use Export) or Category 1-9 (Other Dual-Use Export)

In case no restrictions on destinations, no license required

Determine if the end-user of the export is sanctioned by national or international sanction regulations (links to blacklisted parties)

Is the End-user blacklisted?

Is destination outside of EU?

Is destination a sanctioned country?

Identify the nature of the export: military or dual-use
- Check the required documentation MLA (Multilateral Agreement) and TAA (Technical Assistance Agreement)
- Identify whether a general license is available within <Company> with Export Compliance

Documentation available?

Request a specific license for exporting this item via Export Compliance Contact within <Company>

Export Compliance contact contacts the Ministry of Foreign Affairs within the country of exporting

Document MLA/TAA (general of specific) license in file XX

License acquired?

No export possible, exception for medical purposes

Continue export

No export possible

License acquired?

Needs a specific license

References
2) Category 1-9 Dual-Use Goods
   a. Materials, chemicals, microorganism and toxins
   b. Materiel Processing
   c. Electronica
   d. Computers
   e. Telecommunication and information security
   f. Sensors and lasers
   g. Navigation and avionics
   h. Marine
i. Aerospace and propulsion
3) Link to EU, UN, OFAC etc. sanctioned countries and parties Internal/External lists
## Work Packages: Sanctions and Embargo Screening

### Objectives

- Assess current sanction and embargo procedures and policy
- Gain a view on the countries and regions in scope
- Gain a view on the system landscape and the possibility to automate screening

### Approach

- Research on applicable legislation and company policy (e.g. restricted countries)
- Map the existing IT landscape in view of screening: where is master data maintained, where are orders processed,…
- Define a screening methodology for future automated use, looking at the different scenarios

### Deliverables

- Validated scope definition in view of screening
- Fit gap analysis for system support
- IT Design and Roadmap with requirements (short list requirements)

### Preparations and Scoping

- Desk research
  - Regions and countries in scope
  - Gather company, EU an legal requirements
  - Current system and data management landscape

### Review

- Input Risk assessment
- Policy and Procedure
- List screening requirements (transactional periodical, …)
- Define system support requirements & Fit-Gap analysis
- Input EC Classification (IT)

### Roadmap

- IT Roadmap with requirements
Restricted Party Screening
Industry Practices

Nick Moris
28 April 2015
Restricted Party List Screening
Screening tool implementation approach

• There is no ‘one size fits all’ when it comes to implementing a screening programme.
• Many companies have good practices, but they all do something different depending on their industry, size, footprint and profile.
• The key to effectively implementing a screening tool is a reliable operating model
• Broad considerations include:

1. Jurisdictions a company is doing business
2. Extra-territorial jurisdiction
3. Readiness of BUs to participate
4. Centralized or decentralized model
Restricted Party List Screening
Considerations for your operating model

• When selecting a screening technology solution, it is important to consider the operating model to be used to effectively use that solution.

• It is important to understand how each of the factors can impact:
  • How you conduct screening
  • How often you screen
  • What you screen
  • What you screen against

Risk Matrix per Business Unit
Restricted Party List Screening
Developing your policy

• A screening policy is the linchpin of an effective screening programme. The policy should clearly articulate:

• **Communicating** your policy:
  - The policy should be maintained, updated and disseminated by the Trade Compliance function
  - The policy should be issued to each compliance team responsible for screening
  - The policy should be made available to all senior management, sales and customer facing personnel

[Diagram with bullet points]

Details of the data elements that will be screened (name, legal entity, address, country etc.);
Your risk matrix for identifying who should be screened and how often;
Who is responsible for conducting and releasing screening;
How false positives will be investigated and released;
How holds will be managed and released;
How positive hits will be investigated, decisions made, documented and communicated.
Restricted Party List Screening
Developing your resource capability

• Typically, a company will conduct screening **centrally**:
  − By Business Unit or at Corporate level
  − Via shared service centres (or offshore resource)
  − By Trade Compliance personnel
  − Differently by geography depending on the nature of the business and the required frequency of screening

• Allocating adequate resource:
  − Can depend on the **process** and **tool** you will use
  − Aim to utilize staff with an **existing** compliance or quality **experience**
  − **Skills** necessary include analytical research and investigation skills, report creation and communication skills
  − Avoid a **conflict of interest**
Restricted Party List Screening
Determining who should be screened and how often

- The screening scope can depend upon the **nature** of the business, when in the **lifecycle** you are conducting screening and how business partners and other 3rd party **data** is managed across your business.
- Data elements to screen against can depend on the capability of the tool you use but should typically include **name** (individual, organization, etc..) and **city** or **country**.
- The result may be **multiple screening processes** if you are on multiple platforms:

<table>
<thead>
<tr>
<th>Business Unit 1</th>
<th>Batch Screening</th>
<th>Transactional Screening</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Daily</td>
<td>Monthly</td>
</tr>
<tr>
<td><strong>Customers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prospective Customers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Customers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existing Customers</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Suppliers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product suppliers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Services suppliers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Banks and other financial institutions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logistics providers and other supply chain partners</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local office suppliers (stationary, catering, furniture)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agencies (recruitment/contractors, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Employees (subject to local law discrimination laws)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Employees</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existing employees</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractors</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Restricted Party List Screening
Managing hits – positive and false positive hits

- It is important to have a defined approach for handling any hits that represent partial or complete matches. For example:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and country do not match</td>
<td>False match</td>
</tr>
<tr>
<td>Name partially matches but country does not</td>
<td>Possible false match</td>
</tr>
<tr>
<td>Name partially matches and country matches</td>
<td>Potential positive match, requires investigation and escalation</td>
</tr>
<tr>
<td>Name and country match</td>
<td>Positive match, requires escalation</td>
</tr>
</tbody>
</table>

- Your process should outline:
  - Screening determination **criteria** (name & country, or name, address & country etc.);
  - **Escalation** process for potential positive matches and investigation approach;
  - **Communication** of confirmed positive matches and termination of business partners;
  - **Governance** of who can release blocks.

- The process should be communicated effectively to all relevant personnel.
Restricted Party List Screening

Escalation process

• When reviewing a potential positive hit, the assessment process should include:
  − Conducting additional due diligence
  − Reviewing the source reference
  − Concluding on the likelihood of the hit while considering the legal and reputational risks

• In some companies, responsible parties for making the final decision include:
  − Trade Compliance Director;
  − Chief Compliance Officer;
  − General Counsel;
  − Senior Management of the Business Unite;
  − A combination of some/all of the above.

• Where an active prospect must be discontinued or a customer must be terminated, the Business should work with the Trade Compliance team to notify the customer, terminate the services, and deactivate the customer account in the relevant systems (CRM, ERP etc.).
Restricted Party List Screening
Managing internal conflicts

• Regulators expect **consistency** on **when** and against what **criteria** business partners are screened.
• Companies should seek to deploy a **global standard solution** to manage RPL requirements.
• If not possible, the deployment approach should:
  − Seek to maintain **consistency** at a country and business unit level
  − Have a clear **escalation** point and **across** business units globally

• Regulators typically **recognize** that:
  − Different business units and legal entities may be subject to different regulatory requirements
    - a Japanese entity vs a European entity vs an American entity;
  − Some businesses may require an automated screening solution based on volume of transactions and business partners while others do not;
  − Some businesses need to take a phased approach to deploying a global automated screening solution given the size and readiness of the business units.
Restricted Party Screening: Industry practices
Questions

Nick Moris
Partner
Customs & Global Trade

nmorris@deloitte.com
+ 32 497 05 12 19
Data protection in an era of hackers and internet-spies

Control your data before others do

Luc Beirens
28 April 2015
Agenda

Data as export controlled element

Know the world

Know the enemy

Know the solutions
Data as export controlled element
Technical data in digital format

An export controlled element

• **Technical data typically includes:**
  - Information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles and dual-use items
  - Includes blueprints, drawings, photos, plans, instructions, documentation, and software directly related to defense articles and dual-use items
  - Including specific software for protection and encryption of information

• **Technical data typically does not include:**
  - Basic marketing info on function or purpose or general system descriptions of defense articles
  - General scientific and engineering principals taught in schools, colleges and universities
  - Information in the “public domain”
Information flows in cyber space

Part of the controlled export transfers

*Intangible export includes*

- electronic transfer of data via e-mail, fax, etc of technical data to a destination outside the country / territory
- server access to technical data from a destination outside of the country / territory
Causes of prohibited export of technical data

Just some examples

- **Intentional act**
- **Unintentional data leakage**
  - Lost / stolen data carriers
  - Badly addressed transfers
  - Bad user access management
  - Hacking into servers

With the right information controls most cases can be prevented, detected, acted upon
Incidents
Same goals
New technologies
US charges Chinese hackers for obtaining military data from Boeing, Lockheed Martin

- By Dante D'Orazio
- on July 13, 2014 06:42 pm

The US government is continuing its efforts to put pressure on Chinese cyber-espionage activities. According to The Wall Street Journal, the US Justice Department filed charges against a Chinese national living in Canada named Su Bin. The business owner is charged with working with two anonymous hackers to illegally obtain information on military aircraft produced by US defense contractors.

The three conspirators allegedly worked from 2009 to 2013 on obtaining the information, and they were apparently successful in stealing some sensitive documents related to the Lockheed Martin-built F-22 and F-35 fighter jets, as well as Boeing's C-17 military transport aircraft. The complaint additionally alleges that the conspirators provided Bin with a 1,467-page document of potential hacking targets. Bin could then select attractive files that he could then potentially sell to state-owned aerospace companies in China.

**HACKERS ABLE TO OBTAIN INFO ON F-22 AND F-35 FIGHTER JETS**

The full extent of the connection between Bin's efforts and Chinese-supported hacking remains unclear — it appears that he was working with his own commercial gain in mind, though the data he obtained may have very well ended up in the hands of companies owned by the state. Bin was reportedly arrested in Canada on June 28th, and is facing extradition.

Earlier this year the US charged Chinese army hackers for economic espionage, the first time it formally accused another country of hacking for economic gain. That was merely a high water mark in what has long been a heated exchange of words, as the US has repeatedly cautioned the Chinese over the dangers of its cyber-espionage programs. According to a national intelligence report, the country's efforts to steal US trade secrets are the most aggressive in the world. Estimates say that these cyber-espionage activities cost the US anywhere from $24 billion to $120 billion per year.
Iran hackers target airlines, energy, defense companies - researchers

BOSTON | BY JIM FINKLE

Dec 2 (Reuters) - Iranian hackers have infiltrated major airlines, energy companies, and defense firms around the globe over the past two years in a campaign that could eventually cause physical damage, according to U.S. cyber security firm Cylance.

The report comes as governments scramble to better understand the extent of Iran's cyber capabilities, which researchers say have grown rapidly as Tehran seeks to retaliate for Western cyber attacks on its nuclear program.

"We believe that if the operation is left to continue unabated, it is only a matter of time before the team impacts the world's physical safety," Cylance said in an 87-page report on the hacking campaign released on Tuesday.

The California-based company said its researchers uncovered breaches affecting more than 50 entities in 16 countries, and had evidence they were committed by the same Tehran-based group that was behind a previously reported 2013 cyber attack on a U.S.

---

TRENDING ON REUTERS

U.S. Navy sends more warships near Yemen in security move | VIDEO

---

© 2015 Deloitte Academy
French international broadcaster TV5Monde hacked by 'Islamic State'

French international broadcaster TV5Monde has been hacked by individuals claiming to support "Islamic State." The network was unable to broadcast from any of its channels or social media sites for several hours.

French international television network TV5Monde was hacked by individuals claiming to belong to the self-titled "Islamic State" group (IS) on Wednesday night. The broadcaster temporarily closed its##
Know the world
New technologies
New vulnerabilities
New technologies bring new risks

- Cloud & Virtualization
- Collaboration Platforms
- Internet of things
- Mobile BYOD
- Big data
- Social media
- New payment systems
- Big data
- Social media
The criminal’s toolbox

How does he get in?
Tools of the cyber criminals

An overview

MALWARE
- Generic Malware
- Targeted Malware

BOTNETS
- External botnet
- Internal botnet

SOCIAL ENGINEERING
- Role of social media
- Focused on individual situation

CYBER INTELLIGENCE
- Vulnerabilities & Zero day exploits
- Your infrastructure architecture
**Advanced**
- Targeted: specifically designed for your infra (config files)
- Built in stages – often in RAM
- Own encrypted network & storage protocols
- Anti-forensic: no logging, clean up & self destructing

**Persistent**
- Focus on Servers & Sysadmin's workstations
- Command & Control server(s) in your network
- Different ways out to the internet
- Anti-detection: cmds do not show processes / connections
- Sometimes autopropagation: large-scale network infection

**Threats**
- Read / Write / Delete / Copy / Store / Configure / (Ab)Use
- Spying on Data / Communications => exfiltration of data
- Control (potentially sabotage) infrastructure

**APT's: High end malware – where is the ROI?**
Get in & control unnoticed hacked network over long period
Get / remain in control of your data
Information security characteristics

On which to focus to optimize export control

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non repudiation
- Accountability
Challenges for firms engaged in controlled export

What first?

- Very wide range of security products
- ICT staff often not enough specialized in security issues
- Limited budget
- How good are we protected?
- Should we improve some capabilities?
- How to determine the priorities?
Cyber resilience assessment
A comprehensive approach to determine the way forward

Stakeholders

Cyber Threat Model
Threats
- Phishing towards customers
- Phishing towards persons internal to the organisation
- Targeted malware against customers
- Targeted malware against employees/internal systems

Scenarios

Actors
- Governments
- Terrorists
- Hacktivists
- Criminal organisations
- Competitors

Business Services

Organisational structure

BU1
- Business service 1
- Business service 2
- Business service 3

BU2
- Business service 1
- Business service 2

BU3
- Business service 1
- Business service 2
- Business service 3
- Business service 4

BU4
- Business service 1
- Business service 2
- Business service 3

Communication channels & characteristics

Cyber Resilience Framework

Target Operating Model

© 2015 Deloitte Academy
Data as a controlled element

Questions

Luc Beirens
Director
ERS
lbeirens@deloitte.com
+ 32 475 36 48 73
Export Controls

Sanctions

Alexander Baert
28 April 2015
Export Control Sanctions

Agenda

Introduction 3
Legal Framework 7
Sanctioning Mechanisms 12
Cooperation between Member States 17
What will the future bring? 22
Voluntary Self-Disclosures 26
US Sanctions 30
Introduction
Export Control Sanctions

Introduction

Exhibits of the plea offer:

(h) Schlumberger Ltd. represents that it has implemented and will continue to implement and maintain throughout the term of probation a compliance and ethics program designed to prevent and detect violations of sanctions pursuant to IEEPA and applicable U.S. export control laws throughout its operations, including those of its subsidiaries, divisions, segments, and affiliates. Implementation of these policies and procedures shall not be

(i) Schlumberger Ltd. agrees to retain an independent, third-party compliance consultant (the “Consultant”) to review and assess in a professionally independent and objective fashion Schlumberger Ltd.’s processes, policies, and procedures related to compliance with sanctions pursuant to IEEPA (“Sanctions Policies and Procedures”) and the non-privileged sanctions trade compliance audits conducted by Schlumberger Ltd.’s internal audit function (“Sanctions Audit Reports”). Schlumberger Ltd. agrees that it will retain the Consultant for the purpose of conducting the Consultant’s Reviews as described
Defendant Barclays Bank PLC ("Barclays"), a financial institution registered and organized under the laws of England and Wales, as authorized to specifically act and a criminal forfeiture proceeding, Barclays hereby agrees to pay to the United States the sum of $149,000,000 (the "Forfeiture Amount"). Barclays hereby agrees that the funds paid by Barclays pursuant to this Agreement shall be considered substitute res for the
Export Control Sanctions

Introduction

(h) Barclays must implement compliance procedures and training designed to ensure that the Barclays compliance officer in charge of sanctions is made aware, in a timely manner, of any known requests or attempts by any entity (including, but not limited to, Barclays’ customers, financial institutions, companies, organizations, groups, or persons) to withhold or alter its name or other identifying information where the request or attempt appears to be related to circumventing or evading U.S. sanctions laws. Barclays’ Head of Compliance and Regulatory Affairs, or his or her designee, shall report to the United States the name and contact information of any entity that makes such a request;
Legal Framework
Export Control Sanctions
Legal Framework

Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items


- **Obligation on all Member States to maintain effective national enforcement mechanisms**
- **Obligation on all Member States to have either criminal or civil penalties for violations of export control laws**
- **National law enforcement mechanisms exposed to scrutiny at the international level**
- **Reporting requirements on the national measures to the 1540 Committee**
Export Control Sanctions
Legal Framework

Relevant Considerations in Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items:

- **Consideration 4:** The existence of a common control system and harmonised policies for enforcement and monitoring in all Member States is a prerequisite for establishing the free movement of dual-use items inside the Community.

- **Consideration 13:** In order to ensure that this Regulation is properly applied, each Member State should take measures giving the competent authorities appropriate powers.
Export Control Sanctions
Legal Framework

…each Member State should take measures…

Implications:

- Sanctions and enforcement are regulated by national laws
- Patchwork of sanctions, criminal and administrative procedures
- Substantial differences
- Different cultures
Export Control Sanctions
Legal Framework

…giving the competent authorities appropriate powers…

• Who are the competent authorities?
  – Customs Authorities
  – Authorities issuing the authorizations
Sanction mechanisms
Export Control Sanctions
Sanction mechanisms

What is sanctioned?

- Absence of an authorization
- Expired authorization
- Invalid authorization
- False or fraudulent authorization
# Export Control Sanctions

## Sanction mechanisms

<table>
<thead>
<tr>
<th>Administrative enforcement</th>
<th>Criminal enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Audits</td>
<td>• Investigations by Customs Authorities, who can in most EU Member States conduct criminal investigations with extensive investigative powers or a Prosecutor</td>
</tr>
<tr>
<td>• Withdrawal of licenses</td>
<td>• Prosecution and appearance before a criminal court</td>
</tr>
<tr>
<td>• Administrative fines</td>
<td>• Criminal fines – imprisonment – seizures/confiscation/forfeiture</td>
</tr>
</tbody>
</table>
## Export Control Sanctions

### Sanction mechanisms

Factors taken into account determining an appropriate penalty:

<table>
<thead>
<tr>
<th>General Factors</th>
<th>Mitigating Factors</th>
<th>Aggravating Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Destination of the export</td>
<td>• Voluntary self-disclosure</td>
<td>• Deliberate effort to hide or conceal violations</td>
</tr>
<tr>
<td>• Degree of willfulness involved in violations</td>
<td>• Effective export compliance program</td>
<td>• Serious disregard for export compliance responsibilities</td>
</tr>
<tr>
<td>• Number of violations</td>
<td>• Cooperation with and assist</td>
<td>• Item is significant due to its sensitivity or reason for control</td>
</tr>
<tr>
<td>• Criminal charges</td>
<td>• Criminal charges</td>
<td>• History of violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• High quantity or value of exports</td>
</tr>
</tbody>
</table>
Export Control Sanctions
Sanction mechanisms

Prosecution in Belgium

- Customs Authorities, who have very extensive investigative powers
- Penalties equivalent to half the value or the full value of the goods AND forfeiture of the goods (Art. 10 Law of 11 September 1962 on the import, export and transit of goods and related technology *iuncto* Art. 231 General Law on Customs and Excises)
Cooperation between Member States
Export Control Sanctions

Cooperation between Member States

Article 19 Regulation (EC) No 428/2009:

(1) Member States, in cooperation with the Commission, shall take all appropriate measures to establish direct cooperation and exchange of information between competent authorities, in particular to eliminate the risk that possible disparities in the application of export controls to dual-use items may lead to a deflection of trade, which could create difficulties for one or more Member States.

(2) Member States shall take all appropriate measures to establish direct cooperation and exchange of information between competent authorities with a view to enhance the efficiency of the Community export control regime.
Export Control Sanctions
Cooperation between Member States

• Council Act 98/C of 18 December 1997 drawing up, on the basis of Article K3 of the Treaty on European Union, the Convention on mutual assistance and cooperation between customs administrations (OJ C 24 of 23.01.1998)

• Explanatory report 98/C on the Convention drawn up on the basis of Article K.3 of the treaty on European Union, on mutual assistance and cooperation between customs administrations (OJ 189 of 17.01.1998)

• Agreements on cooperation with third countries
Export Control Sanctions
Cooperation between Member States

Customs Information System (CIS)
• Centralised system to facilitate cooperation in combating customs-related crime
• Developed and managed by the European Anti-fraud Office (OLAF)
• Databases with information on
  – Commodities
  – Means of transport
  – Businesses
  – Persons
  – Fraud trends
  – Availability of expertise

Export Control System (ECS)
• Risk analysis for safety purposes (Art. 264 UCC)
• Information European-wide accessible for customs authorities
  – Results of inspections of export consignments
  – Confirmation that consignments left the EU
Export Control Sanctions
Cooperation between Member States

Right of intervention for goods in transit for export via a Member State, if an export authorization is granted by another Member State?

- ECJ 4 October 1991, Richardt, C-367/89:
  … it is common ground that the importation, exportation and transit of goods capable of being used for strategic purposes may affect the public security of a Member State, which it is therefore entitled to protect

- ECJ 17 October 1995, Leifer, C-83/94:
  … a Member State may, exceptionally, adopt national measures restricting the export of dual-use goods to non-member countries on the ground that this is necessary in order to prevent the risk of a serious disturbance to its foreign relations or to the peaceful coexistence of nations which may affect the public security of a Member State…
What will the future bring?
Export Control Sanctions
What will the future bring?

• Enforcement has long been neglected in Europe, in contrast to the USA

• Efforts to strengthen export control enforcement are building up

• The Review of the export control policy (24 April 2014 – COM(2014)244)
  • Consistent implementation and enforcement across the EU is essential
  • With over 40,000 applications per year export controls become demanding
  • Enhancement of structured exchange of information
  • Enhancement of strategic and operational cooperation with enforcement agencies (i.e. customs)
  • Improvement of coherence between different EU institutions
Export Control Sanctions

What will the future bring?

- Policy of Belgian Customs Authorities 2015 – 2019

The Customs Authorities play an important role in controlling the import and export of dual-use goods, weapons, ammunition, explosives, weapons of mass destruction, ozone depleting substances and radioactive substances. The investigative services of the Customs Authorities play an important role in the treatment of sensitive information and signals relating to aforementioned goods. These signals, given their potential consequences, cannot be ignored and require discreet investigation. The national and international cooperation with a number of agencies such as foreign security is paramount.

Action Point: Increased bill of lading / manifest screening incoming and outgoing shipments via sea and airports.

Timing: Continuous

To do: Additional use of detection equipment at ports, airports and logistics centers. To this end, targeted work sheets developed by the service working methods of the administration TCV.

Timing: Continuous

Action point: Targeted information exchange.

Timing: Continuous
Obstacles for an EU-wide sanction/enforcement system?

- The ultimate power to criminalize conduct is legitimized by the will of the people in democratic states
  - European Parliament not a democratic institution?
- Variety of legal traditions
- Cry for EU-wide sanction/enforcement system gets louder

  *The absence of an EU framework for the imposition of customs sanctions damages the foundations of the EU. It creates serious difficulties for the EU both externally and internally. It also creates serious difficulties for commercial operators and undermines the ability of officials to enforce EU law in general and to combat counterfeiting in particular. Accordingly, the creation of an EU framework is very much to be encouraged.*
Voluntary Self-Disclosures
Export Control Sanctions
Voluntary Self-Disclosures

• In the US are voluntary self-disclosures a current practice
  − Regulated process
  − Regulated fines and penalties

• In the EU, the use of voluntary self-disclosures depends from country to country

• A voluntary self-disclosure does not prevent prosecution!
Export Control Sanctions
Voluntary Self-Disclosures

- Beneficial for (the future) relationship with the authorities (Trustworthiness / AEO)
- Mitigating factor – reduction or exemption of penalties
- Active involvement in investigations which can give you power of guidance
- M&A transactions – cleansing of the merged / acquired company
Export Control Sanctions
Voluntary Self-Disclosures

• Preparation is key
  • Thorough investigations of the facts
  • Thorough investigations of all relevant data and documents
  • In dialogue with all stakeholders

• Presentation of the facts
  • Fully and honest
  • What / when / where / why?
  • Most important: elimination of risks towards the future
    – Compliance programs
US Sanctions
## Export Control Sanctions

### US Sanctions

<table>
<thead>
<tr>
<th>The Export Administration Regulations (EAR)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criminal Sanctions</strong></td>
</tr>
<tr>
<td>• Fines of 1,000,000 USD or five times the value of the exports for each violation</td>
</tr>
<tr>
<td>• Imprisonment for up to 10 years</td>
</tr>
<tr>
<td><strong>Civil Sanctions</strong></td>
</tr>
<tr>
<td>• Fines of 120,000 USD per violation</td>
</tr>
<tr>
<td>• Denial of export privileges</td>
</tr>
<tr>
<td>• Exclusion from practice</td>
</tr>
<tr>
<td>• Seizure/Forfeiture of goods</td>
</tr>
</tbody>
</table>
# Export Control Sanctions

## US Sanctions

### The International Emergency Economic Powers Act (IEEPA)

| **Criminal Sanctions**       | • Fines of 1,000,000 USD for each violation  
|                             | • Imprisonment for up to 20 years |
| **Civil Sanctions**          | • Fines of 250,000 USD per violation or twice the value of the transaction  
|                             | • Denial of export privileges  
|                             | • Exclusion from practice  
|                             | • Seizure/Forfeiture of goods |
Export Control Sanctions
US Sanctions

The International Traffic in Arms Regulations (ITAR)

<table>
<thead>
<tr>
<th>Sanctions</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criminal Sanctions</strong></td>
<td>• Fines of 1,000,000 USD for each violation  &lt;br&gt; • Imprisonment for up to 10 years</td>
</tr>
<tr>
<td><strong>Civil Sanctions</strong></td>
<td>• Fines of 500,000 USD per violation  &lt;br&gt; • Denial of export privileges  &lt;br&gt;    • Seizure/Forfeiture of goods</td>
</tr>
</tbody>
</table>
# Export Control Sanctions

## US Sanctions

<table>
<thead>
<tr>
<th>The Office of Foreign Assets Control (OFAC)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criminal Sanctions</strong></td>
</tr>
<tr>
<td>• Fines of 1,000,000 USD for each violation</td>
</tr>
<tr>
<td>• Imprisonment for up to 20 years</td>
</tr>
<tr>
<td><strong>Civil Sanctions</strong></td>
</tr>
<tr>
<td>• Fines of 55,000 USD per violation</td>
</tr>
<tr>
<td>• Seizure/Forfeiture of goods</td>
</tr>
</tbody>
</table>
Export Control Sanctions
US Sanctions

- The US legislative instruments have extra-territorial application: any company that conducts business in violation with US export control regulations risks US export enforcement
- In breach of international law
- In 2012 ING Bank N.V. (The Netherlands) was forfeited 619,000,000 USD for processing the financial aspects of unlawful exports between a Dutch company to Cuba and Iran
Conclusion:

A strong compliance program, robust compliance procedures, safeguards and trainings are essential.
Export Control Sanctions
Questions?

Alexander Baert
Lawyer
abaert@laga.be
Tel. +32 2 800 71 51
Export Controls

Wrap up
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s more than 200,000 professionals are committed to becoming the standard of excellence.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2014. For information, contact Deloitte Belgium