### Obligations & Risks

#### INCOTERMS® 2010 Rules

<table>
<thead>
<tr>
<th>Term</th>
<th>Seller's Obligations</th>
<th>Buyer's Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXW</td>
<td>Seller bears all costs and risks up to the border of the ship</td>
<td>Buyer bears all costs and risks from the border of the ship</td>
</tr>
<tr>
<td>FCA</td>
<td>Seller bears all costs and risks up to the named place</td>
<td>Buyer bears all costs and risks from the named place</td>
</tr>
<tr>
<td>CPT</td>
<td>Seller bears all costs and risks up to the named place</td>
<td>Buyer bears all costs and risks from the named place</td>
</tr>
<tr>
<td>CIP</td>
<td>Seller bears all costs and risks up to the named place</td>
<td>Buyer bears all costs and risks from the named place</td>
</tr>
<tr>
<td>DAP</td>
<td>Seller bears all costs and risks up to the named place</td>
<td>Buyer bears all costs and risks from the named place</td>
</tr>
<tr>
<td>DDP</td>
<td>Seller bears all costs and risks up to the buyer's premises</td>
<td>Buyer bears all costs and risks from the buyer's premises</td>
</tr>
</tbody>
</table>

---

**Responsibility**

- **U.S.A. IMPORT**: Seller bears responsibility for import duties.
- **U.S.A. EXPORT**: Buyer bears responsibility for export duties.
The 11 key components of a data protection strategy include:

1. **Data Policy and Governance**
   - Establish clear data protection policies and guidelines.
   - Ensure all employees are trained on data protection practices.

2. **Data Classification**
   - Categorize data based on sensitivity and importance.
   - Implement access controls based on data classification.

3. **Data Encryption**
   - Encrypt data both at rest and in transit.
   - Use strong encryption algorithms and protocols.

4. **Data Backup and Recovery**
   - Implement robust backup and recovery strategies.
   - Test recovery procedures regularly.

5. **Data Integrity and Authentication**
   - Ensure data integrity through checksums and other methods.
   - Use strong authentication mechanisms for data access.

6. **Data Loss Prevention**
   - Implement measures to prevent data loss.
   - Monitor for suspicious activity.

7. **Data Retention Policies**
   - Define retention periods for data.
   - Ensure adherence to legal and regulatory requirements.

8. **Data Breach Notification**
   - Establish procedures for data breach notification.
   - Train employees on data breach response.

9. **Compliance with Data Protection Laws**
   - Stay updated with data protection laws and regulations.
   - Ensure compliance with all applicable laws.

10. **Data Access Controls**
    - Implement access controls for data.
    - Limit access based on roles and responsibilities.

11. **Data Protection Compliance and Auditing**
    - Regularly audit data protection measures.
    - Ensure ongoing compliance with data protection frameworks.

Implementing these components will help organizations effectively manage and protect data, ensuring compliance with regulations and minimizing data breaches.