<table>
<thead>
<tr>
<th>INFUENCERS (EXTERNAL &amp; INTERNAL)</th>
<th>POLICIES</th>
<th>CONTROL OBJECTIVES</th>
<th>STANDARDS</th>
<th>GUIDELINES</th>
<th>PROCEDURES</th>
<th>CONTROLS</th>
<th>METRICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>It all starts with external influencers – these establish what is considered to be due care for information security operations. These are both statutory requirements (laws), regulatory requirements (government regulations) and contractual requirements (legally-binding agreements) that companies must address. External influencers usually impose meaningful penalties for non-compliance. External influencers are non-negotiable and are the primary source for defining a need for a policy and for establishing control objectives. Internal influencers focus on management’s desire for consistently efficient and effective operations: - Business strategy - Goals &amp; objectives: - Customer satisfaction - Service levels - Budget constraint - Quality levels</td>
<td>Policies</td>
<td>Control Objectives</td>
<td>Standards</td>
<td>Guidelines</td>
<td>Procedures</td>
<td>Controls</td>
<td>Metrics</td>
</tr>
<tr>
<td>Corporate Policies &amp; Directives</td>
<td>Every Control Map To A Control Objective</td>
<td>Baseline Configuration Requirements</td>
<td>Every Standard Map To A Control Objective</td>
<td>Policies Support Applicable Standards</td>
<td>Procedures Support Applicable Standards</td>
<td>Policies Support Applicable Standards</td>
<td>Policies Support Applicable Standards</td>
</tr>
<tr>
<td>Contractual</td>
<td>PCI/DSS</td>
<td>Every Control Map To A Standard</td>
<td>Controls</td>
<td>Metrics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA, NIST 800-171, FedRAMP, FACTA COPPA</td>
<td>Statutory / Regulatory (US)</td>
<td>Baseline Configuration</td>
<td>Controls</td>
<td>Maps To A Standard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statutory / Regulatory (Non-US)</td>
<td>EU GDPR Data Protection Act (UK) Int Data / Privacy Laws</td>
<td>Legal Requirements / ISO 27002 / NIST 800-53</td>
<td>Policies</td>
<td>Maps To A Standard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal Requirements / ISO 27002 / NIST 800-53</td>
<td>Legal Requirements / ISO 27002 / NIST 800-53</td>
<td>Legal Requirements / ISO 27002 / NIST 800-53</td>
<td>Policies</td>
<td>Maps To A Standard</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Control Objectives**
- A policy is a formally established requirement to guide decisions and achieve rational outcomes – essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures. External influencers are commonly the root cause for a Policy’s existence.
- Control Objectives are targets or desired conditions to be met that are designed to ensure that policy exists in the environment.
- Where applicable, Control Objectives are directly linked to an industry-recognized best practice to align IT security with accepted Due Care requirements.

**Standards**
- Standards are formally established requirements in regard to processes, actions, and configurations that satisfy Control Objectives.

**Guidelines**
- Guidelines are recommended practices that are based on industry-recognized best practices. Guidelines help augment Standards when discretion is permissible.

**Procedures**
- Procedures are a formal method of doing something, based on a series of actions conducted in a specific order or manner.

**Controls**
- Controls are technical or administrative safeguards that map prevent, detect or lessen the impact of threats meant to exploit a vulnerability.

**Metrics**
- Metrics are designed to facilitate decision-making, improve performance, and improve accountability through the collection, analysis, and reporting of relevant performance-related data.

**Top-down Integration of**
- Digital Security Governance & Support Based on Leading Practices

**Bottom-up Integration of**
- Digital Security Governance & Support Based on Leading Practices

**External Influencers**
- Establish Reasonable Expectations

**Internal Influencers**
- Drive Policies & Control Objectives (Compliance Oriented)

**Policies Define Expectations & Scope Control Objectives**

**Standards Enforce Control Objectives**

**Guidelines Support Control Objectives**

**Procedures Support Standards & Establish Control Activities**

**Control Testing Measures Compliance With Standards**

**Controls Support Standards**

**Metrics Support Digital Security Governance For Due Diligence**