A top-down approach to enterprise security architecture can be used to build a business-driven security architecture. An approach to prioritizing the security projects that are identified as part of architecture assessment while ensuring business alignment follows.

Business risk and attributes can be used to identify relevant security controls and a maturity assessment can be performed to identify the current and desired maturity level of those controls and build an action plan. The steps can be summarized as follows:

1. Select a security framework that is relevant to business such as those developed by the Payment Card Industry (PCI), the US National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO).

2. Understand and document business goals and attributes.

3. Identify the framework controls that are relevant to business and can be verified by business risk.

4. Adjust and customize the controls based on business requirements and operation.

5. Perform a gap analysis and maturity assessment to identify what is missing or incomplete.

6. Develop a program to implement the missing or incomplete controls.

Figure 1 is a summary of these steps and a visual representation of the architecture life cycle.

Architecture Framework and Gap Assessment

Using frameworks such as COBIT® or ISO 27001 can help identify a list of relevant security controls that can be used to develop a comprehensive security architecture that is relevant to business.

COBIT® 5 for Information Security covers the services, infrastructure and applications enabler and includes security architecture capabilities that can be used to assess the maturity of the current architecture.

Figure 2 illustrates an example of how service capabilities and supporting technologies in COBIT can be used to build a security architecture framework and controls. All identified controls should relate to business risk and attributes.

Maturity Assessment

Once the security architecture framework is developed and the gaps are identified, the next step is to create an implementation plan and specify priorities. This would normally be a long-term program, depending on the size and budget of the organization. This is an important step in the
Risk Management

Risk is commonly categorized into two categories: business risk and operational risk. While business risk is identified by the business and used to define security architecture controls, operational risk includes threats, vulnerabilities and new audit findings, and managing those can complement the controls that are already in place. Figure 4 offers a view of information security risk sources, including business risk vs. operational risk.

Information security risk is normally calculated using qualitative or quantitative methods. Risk assessment techniques such as The Open Group Open FAIR® can be used to assess the likelihood

<table>
<thead>
<tr>
<th>Identified Control</th>
<th>Current Maturity Level</th>
<th>Desired Maturity Level</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-point malware protection</td>
<td>1</td>
<td>3</td>
<td>• Fifty percent of machines lack malware protection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• A host-based intrusion prevention system (HIPS) is not enabled on end points.</td>
</tr>
<tr>
<td>Data loss prevention (DLP)</td>
<td>0</td>
<td>2</td>
<td>• There is no DLP solution in place.</td>
</tr>
<tr>
<td>Disaster recovery (DR) plan</td>
<td>1</td>
<td>3</td>
<td>• The DR plan is not practiced.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The DR plan is not updated on a regular basis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• An offsite communication plan is not available.</td>
</tr>
</tbody>
</table>
and impact of a risk, calculate a risk score, and identify the appropriate mitigation controls to remediate the risk (Figure 5).

While not going into a deep discussion about risk management techniques and how they are done, the goal is to have a heat chart for areas of security risk, calculate a severity level for each and assign a risk score to each based on the severity level. For example, a critical risk would have a score of 5, a high risk would have a score of 4, and so on.

Two important comments should be made about information security risk assessments:

1. Ultimately, all information security risk should be mapped to business risk. Any information security risk that cannot be related to a relevant business risk is not valid and would not be considered business-critical.
A heat chart is then built using the business risk captured in the risk register, and a score assigned to each risk, as explained previously (figure 7).

2. Although it would follow the same logic to prioritize the operational risk, this article focuses on and covers only prioritization of the security controls that were identified as part of the security architecture gap assessment. These controls would be used to remediate high-level business risk and would normally be taken from standard frameworks such as COBIT or those developed by ISO or NIST.

**Architecture Controls Prioritization**

The method used to identify priorities involves a business risk register. Every business has (or should have) a risk register in place. Normally, a business risk register captures overall business risk, its likelihood and impact on business, and a mitigation strategy.

An example of a standard business risk register is shown in figure 6.

A heat chart is then built using the business risk captured in the risk register, and a score assigned to each risk, as explained previously (figure 7).

To bring this into context, the two examples of risk listed in figure 6 will have the risk scores shown in figure 8.
This calculation is used to prioritize the implementation.

To explain this with an example, using the control register table shown in figure 3, figure 9 depicts the linking of the controls to the business risk with already identified scores. In addition, assuming the control is not in place, the information security risk score is calculated separately. For example, if the end point malware protection is not in place, the risk of IP theft is quite high (5).

It should be noted that this is a very simple explanation and risk management techniques such as Open FAIR may need a bit more effort to calculate the risk score, but the approach would stay the same.

Using this method, it is easy to prioritize controls or projects and plan their implementation properly. This is useful expertise in managing the architecture life cycle. It will ensure the alignment of security and business priorities and automatically justify them.

In the example shown in figure 9, the priority of implementing an end-point malware protection system is much higher than having a DLP solution in place.

**Conclusion**

Using a business risk register to prioritize security projects is an appropriate approach that not only justifies the life cycle management of security

<table>
<thead>
<tr>
<th>Identified Control</th>
<th>Relevant Business Risk</th>
<th>Relevant Information Security Risk</th>
<th>Business Risk Score/Impact (1-5)</th>
<th>Information Security Risk Score/Likelihood (1-5)</th>
<th>Overall Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint malware protection</td>
<td>IP theft</td>
<td>Endpoint virus/ Trojan infection</td>
<td>3</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>DLP</td>
<td>IP theft</td>
<td>Unauthorized access to digital IP</td>
<td>3</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>DR plan</td>
<td>Critical IT failure</td>
<td>Unavailability of critical IT services in disaster</td>
<td>4</td>
<td>3</td>
<td>12</td>
</tr>
</tbody>
</table>
projects, but also ensures business alignment and minimizes potential impact.

The essential steps required to ensure that security controls and projects are in alignment with business priorities include:

1. Mapping security controls with business risk scenarios
2. Identifying the information security risk score if the control is not in place
3. Identifying the business risk score for the relevant control
4. Calculating the overall risk score using the formula: Overall risk score = business risk score x information security risk score
5. Prioritizing projects based on the overall risk score

Endnotes

2 Ibid. See the previous article for more details on this process.
4 The Open Group, The Open Group Open FAIR Certification Program, www.opengroup.org/certifications/openfair