A Business Process Approach to Assets and Risks

1. A New Approach ................................................................. 2

2. Asset and Configuration Management ........................................ 2
   2.1. What Is Asset Management?
   2.2. What Is Configuration Management?
   2.3. Defining Criticality of Assets
   2.4. Asset and Configuration Management in the Enterprise

   3.1. Top-Down Approach
   3.2. Bottom-Up Approach
   3.3. The Criticality Challenge with Shared IT Assets

   4.1.1. Business Process Service Levels
   4.1.2. Better Prioritization
   4.1.3. Risk and Security Requirements Profile

5. Conclusion .................................................................................. 4
1. A New Approach
For many years the security industry believed that the best way to protect an enterprise was to contain its data within the perimeter, build the walls, and keep the “bad guys” out. Security was not on the CxO’s agenda, was considered as an IT problem and solutions were developed from a mainly technical point of view. Today, security has changed significantly. The threat landscape has evolved, becoming more sophisticated and targeted. Compliance has become one of the most critical challenges. And new security challenges have been created as enterprises extend their networks and data to other parties, including partners, suppliers and the mobile workforce.

This changing security landscape requires us to take a different approach. Instead of taking an isolated view with respect to assets and risks, we recommend a business process view. This business process view has several advantages, as we will discuss in the remainder of this paper.

2. Asset and Configuration Management
There are different definitions of a business process, but we define it as a combination of interdependent assets and activities, which work together to achieve a predefined goal. Examples of business processes are the enrollment of new employees, receiving/controlling/paying of an invoice, and the provisioning of an online transaction system. Broadly defined, such a process can range from relatively simple activities such as publishing and maintaining information on a public website to more sophisticated processes such as banking transaction systems.

An asset can be defined as anything which has value to an enterprise. An asset can be, for instance, people, furniture, documentation, hardware, and software. For the purpose of this paper, we are concerned with IT assets. Examples of IT assets are user manuals, file servers, mobile devices, laptops, and network and security devices. For example, publishing information on the enterprise’s website can involve a combination of the following (IT) assets:
- People, including web developers and system administrators.
- Hardware, including server platforms, network devices, security devices.
- Software, including operating systems, web servers.
- Documentation, including security hardening guidelines, user manuals, policies and procedures.

The two main processes related to IT assets are asset management and configuration management.

2.1. What Is Asset Management?
To keep track of the IT assets, most enterprises have deployed an IT asset management system. The primary goals of such a system are:
1. To have an inventory of the assets, to assign ownership to the assets and define the rules of acceptable use of the assets.
2. To define the classification of the assets in terms of value, legal requirements, sensitivity, security requirements and criticality to the enterprise (including labelling of information contained in an asset, if applicable).

2.2. What Is Configuration Management?
The primary goals of configuration management are to:
1. Define the different configuration items (CIs) to be used (e.g., hardware, software).
2. Define the configuration management database (CMDB), which stores the CIs details and the relationships between the CIs.

2.3. Defining Criticality of Assets
Although IT asset management and configuration management are different activities or processes, they are also related. It is important and useful to have the individual configurations of IT assets registered in the CMDB (e.g., change management process). It is also important to define the criticality of those IT assets. Both asset management and configuration management can co-exist without any interaction. However, we believe that a combined approach will lead to better qualified decisions, depending on the data available.

For example: an IT asset may be defined as critical (asset management), but if the CMDB (configuration management) shows that it is not vulnerable to certain security threats, those threats can be ignored for that particular IT asset. An isolated approach toward asset and configuration management doesn’t lead to that conclusion, as every security threat will be evaluated in isolation. That is: I know that the IT asset is critical, but I don’t know whether I should be concerned about its vulnerability. Another inconclusive isolated view states: I know that an asset is vulnerable for a certain security threat, but I don’t know whether the asset is critical enough to be concerned about this threat.

2.4. Asset and Configuration Management in the Enterprise
Many enterprises have deployed an IT asset management or a configuration management solution. With respect to those implementations we observe the following:
1. Not all enterprises make a clear separation between IT asset management and configuration management, but if the CMDB (configuration management) shows that it is not vulnerable to certain security threats, those threats can be ignored for that particular IT asset. An isolated approach toward asset and configuration management doesn’t lead to that conclusion, as every security threat will be evaluated in isolation. That is: I know that the IT asset is critical, but I don’t know whether I should be concerned about its vulnerability. Another inconclusive isolated view states: I know that an asset is vulnerable for a certain security threat, but I don’t know whether the asset is critical enough to be concerned about this threat.

3. A Business Process View of Assets and Risks
IT assets are individual entities and knowing which ones you have and what the classifications are has its value. But an IT asset is also part of a business process. It is this view that provides an overall picture with respect to, for example, the risk profile of business processes. The best way to explain our business process view toward assets and risks is by means of an example.

Assume the following two, separate business processes:
1. Online banking [OB] – classified as a highly critical business process
2. Public website [PW] – classified as a medium critical business process
The online banking business process provides customers the ability to access their bank account via the Internet, using a web browser. This is only accessible for authorised and enrolled users. The public website business process publishes information about the enterprise on the enterprise’s website and is accessible for everybody on the Internet.

Below, in Figure 1, we depict a high level overview of the online banking and public website infrastructure:

![Figure 1. OB and PW Infrastructure Overview](image)

The following table describes the IT assets which are used by both business processes:

<table>
<thead>
<tr>
<th>IT Asset</th>
<th>Used by OB</th>
<th>Used by PW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Server (OB-DBS)</td>
<td>Yes – Dedicated</td>
<td>No</td>
</tr>
<tr>
<td>Application Server (OB-APS)</td>
<td>Yes – Dedicated</td>
<td>No</td>
</tr>
<tr>
<td>Switch (OB-S)</td>
<td>Yes – Dedicated</td>
<td>No</td>
</tr>
<tr>
<td>Web Server (PW-WBS)</td>
<td>No</td>
<td>Yes – Dedicated</td>
</tr>
<tr>
<td>Router (R)</td>
<td>Yes – Shared</td>
<td>Yes – Shared</td>
</tr>
<tr>
<td>Firewall (FW)</td>
<td>Yes – Shared</td>
<td>Yes – Shared</td>
</tr>
<tr>
<td>Internet Connection (IC)</td>
<td>Yes – Shared</td>
<td>Yes – Shared</td>
</tr>
</tbody>
</table>

Table 1. IT Assets used by OB and PW

As described in section 2.1, an IT asset has a criticality value. There are (many) different approaches to determine the criticality of an IT asset. The most common or used approaches are the top-down and the bottom-up approach.

### 3.1. Top-Down Approach

The top-down approach starts from the business process view. The criticality of the individual IT assets, which belong to that business process, inherit the business process criticality. This is a rather easy and straightforward approach, but care must be taken in case of shared IT assets—especially when the business processes have different criticality values. If we apply the top-down approach to the OB business process (criticality high), the criticality values of the IT assets belonging to OB are as follows:

<table>
<thead>
<tr>
<th>IT Asset</th>
<th>Individual Asset Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Server (OB-DBS)</td>
<td>High</td>
</tr>
<tr>
<td>Application Server (OB-APS)</td>
<td>High</td>
</tr>
<tr>
<td>Switch (OB-S)</td>
<td>High</td>
</tr>
<tr>
<td>Router (R)</td>
<td>High</td>
</tr>
<tr>
<td>Firewall (FW)</td>
<td>High</td>
</tr>
<tr>
<td>Internet Connection (IC)</td>
<td>High</td>
</tr>
</tbody>
</table>

Table 2. Top-down approach for the OB business process

### 3.2. Bottom-Up Approach

The bottom-up approach is more complicated and time consuming: the IT asset criticality is initially assigned individually and is then (if necessary) aligned with the criticality of the business processes it belongs to. If we apply the bottom-up approach to the PW business process (criticality medium), the criticality values of the IT assets belonging to the public website are as follows:

<table>
<thead>
<tr>
<th>IT Asset</th>
<th>Individual Asset Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server (PW-WBS)</td>
<td>Medium</td>
</tr>
<tr>
<td>Router (R)</td>
<td>Medium</td>
</tr>
<tr>
<td>Firewall (FW)</td>
<td>Medium</td>
</tr>
<tr>
<td>Internet Connection (IC)</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Table 3. Bottom-up approach for the PW business process

The bottom-up approach can become time-consuming and labor-intensive in situations with a considerable number of IT assets (which is the case for most enterprises). A methodology that automatically assigns criticality values to individual IT assets is appreciated.

### 3.3. The Criticality Challenge with Shared IT Assets

The devil is in the details, and for both approaches, the devil is in shared IT assets. If we take our example infrastructure (Figure 1), we see that the shared IT assets are internet connections (IC), router (R), and firewall (FW):

<table>
<thead>
<tr>
<th>IT Asset</th>
<th>Individual Asset Criticality in OB</th>
<th>Individual Asset Criticality in PW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router (R)</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Firewall (FW)</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Internet Connection (IC)</td>
<td>High</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Table 4. Shared IT Assets

As shown in the table above, the IT asset criticality values are different for both business processes.
Essentially (in this case), there are two sides of the coin:

1. Let the public website business process prevail and assign "medium" rating to the shared IT assets. Given the fact that implemented (security) controls and measures should be related to the criticality of the business process, this may lead to a higher risk profile for the online banking business process. Simply because the set of controls and measures for a medium critical business process may be a subset of those for a highly critical business process. For example, for the public website business process, high availability of the infrastructure may not be a requirement or a concern, while this might be the case for the online banking business process.

2. Let the online banking business process prevail because of its higher criticality value and the shared IT assets are assigned a high criticality. In this scenario, the public website business process hitchhikes on the extra implemented controls and measures of the online banking business process and may be considered over-protected in relation to its criticality.

Both scenarios may lead to discussions among business owners, especially when business processes are owned by different owners or departments. For example, the first scenario may not be acceptable for the online banking business owner due to a higher risk profile. The second scenario may not be acceptable by the public website business owner if he/she is also charged for the extra controls.

4. Why Is a Business Process Approach Useful?
A business process approach is useful and has its advantages. For example, it enables a better prioritization of security events and the ability to define service levels, risk, and security profiles at the business process level. We discuss these examples in more detail below.

4.1. Business Process Service Levels
Most service levels as implemented (either internally within enterprises as well as with managed security services providers) are based on individual IT assets. Generated alerts are followed up related to that particular asset in compliance with a pre-defined service level (e.g., a high-priority alert has to be escalated within 30 minutes). Following up alerts from individual assets certainly has its value, but it would be more valuable if we could define service levels for business processes.

The fact that an asset has generated an alert does not mean that this impacts the business process. For example, if the firewall implementation as depicted in Figure 1 is in high-availability mode and the primary firewall fails, this will not (or should not) impact the online banking or public website business processes, as the secondary firewall will take over. An alert will be generated and should be followed up. However, this particular event can be assigned a lower priority as the business processes are still up and running. If we would purely look at the firewall in isolation, such an alert might be considered as a high priority. Less communication and fewer escalations are needed (in terms of number of alerts) when we approach an escalation at the business process level, instead of escalations per individual IT asset.

The business process view is also useful from a compliance perspective. Instead of showing compliance related to individual assets, an enterprise can show compliance with a business process. This is especially important when a business process consists of many individual IT assets as this will save resources.

4.1.2. Better Prioritization
When monitoring events, the business process approach also provides a methodology to prioritize events based on business process criticality instead of individual asset criticality. For example, events from the online banking business process (regardless which IT asset has generated an event) will get a higher prioritization than events related to the public website business process. This is so because the online banking business process has a higher criticality value than the public website business process. In case of an individual IT asset approach, the usual methodology is first come, first serve. Although events can also be prioritized in that case, the prioritization is still based on individual asset criticality and does not take the overall business process picture into account.

The big advantage is that the business approach allows your security staff to better determine which events should be followed up first. This is especially important when following up events in compliance with critical or tight service levels. It also caters for a more differentiated service level management, whereby prioritized events can be followed up more quickly.

4.1.3. Risk and Security Requirements Profile
In the previous section, we described how we can define and use business process service levels. We can use this approach also for risk and security profiles. We define those profiles on a business process level instead of on the level of individual IT assets.

For the security profile, we evaluate the typical CIA (confidentiality, integrity and availability) security requirements for the business process instead of evaluating those requirements on the level of IT assets. This is the same principle as we discussed in section 3, where we described the criticality values of business processes.

The risk profile for a business process enables an enterprise to build an overall risk picture of, say, critical business processes. Focusing on the risk profile of an individual IT assets provides insight in that particular asset, but not necessarily to the business process(es) it belongs to.

The bottom line is that as long as the business process risk and security profile is acceptable, the IT asset profiles belonging to that particular business process are less important.

5. Conclusion
In this paper, we discussed a business process approach toward IT assets and risks. We described the top-down and bottom-up approach on how to assign criticality values to business processes and IT assets, and explained this concept by means of an example. We also discussed the advantages of the business process approach. Our examples in this paper are simplified in order to convey the business process message first. In reality, the situation can become much more complex. Verizon Business will continue its thought leadership on this and many other security related subjects, and we will publish our results in white papers on a regular basis.

verizonbusiness.com
© 2009 Verizon. All Rights Reserved. WP13406 10/09
The Verizon and Verizon Business names and logos and all other names, logos, and slogans identifying Verizon’s products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.