The Annual Conference on Management and Information Technology (ACMIT) 2016

The Implementation IT Risk Management of Hardware and Software Obsolescence by using ISO27001/ISO 27002 in Pharmaceutical Industry

Heri Rukmana
rukmah@gmail.com

EduTown, BSD City, Tangerang, Indonesia

Abstract

Risk Management is a discipline that exists to deal with non-speculative risks – those risks from which only a loss can occur. Hardware and software obsolescence which are used in pharmaceutical industry equipment are the subject of Risk Management since these obsolescence may cause either a profit or loss and impact to the business strategy, which can reduce the value of the assets with which the organization undertakes its speculative activity.

Keywords : Risk Management, Hardware and Software Obsolescence.

1. Introduction

The electronic industries are one of the very dynamic sectors of the world economy. In the developed country such as United States, these industries have grown three times greater than the overall economy in the last ten years. The semiconductor industry is now the first value-added to the U.S. economy, and the computer and consumer industry segments stunt almost any other market segments. For instances, Intel's market capitalization was higher than the three largest market capitalization of three combination U.S automakers.

Beginning on April 8th, 2014, Microsoft and all other hardware and software companies will discontinue and stop their support of the Windows XP operating system. When it happens, Windows XP will become vulnerable for viruses because antivirus programs will be outdated and stop not updated. New peripheral devices such as a printer, keyboard, or mouse will be unable to connect to the computer since the system does not meet the minimum requirements to run them. HP has already shut off support for Windows XP, and other big brands will follow suit over the course of the year. If you call a retailer or other company for direct support and say you are still running XP, they will be unable to assist you.

With Rapid growth of Technology, rate of obsolescence of hardware and software which are used as components in equipment for pharmaceutical industry has increased. Factor which have impacted obsolescence of hardware and software of electronics components are:
- Advancement in Microcontroller chips
- Number of generic parts with shorter obsolescence cycles
- Rapid evolution of 64 bit computing hardware
- Microsoft’s decision to prepone discontinuation of support for all 32 bit OS

Most of manufacturing systems in pharmaceutical are still in either old PLC/microcontrollers or Windows XP which are no longer available for sale and have limited to no serviceability remaining and support from PLC maker or Microsoft. Hence, pharmaceutical industry has to manage risks which occur due to this obsolescence. The question is “How do we mitigate business loss due to hardware and software obsolescence of manufacturing system in Pharmaceutical Industry?”

2. Methodology

This paper will focus on Obsolescence Management Strategy to mitigate business loss due to hardware and software obsolescence.
The methodology will be used for this paper are as follows:
1. Technology life cycle to identified hardware and software obsolescence.
2. Risk identification, mitigation plan and prioritization matrix of hardware and software obsolescence.
3. Field studies by looking the company’s preparedness of any hardware and software obsolescence.

2.1 Hardware and Software (H&S) Obsolescence Risk Management Process

There are six steps for Hardware and Software (H&S) Obsolescence Risk Management Process as follows (see Picture 1):
2.1.1 Hardware and Software (H&S) identification
2.1.2 Determine H&S Life Cycle
2.1.3 Determine H&S vulnerabilities and threats
2.1.4 Determine H&S criticality
2.1.5 Risk Assessment
2.1.6 Risk Mitigation Strategy

Figure 1. Hardware and Software (H&S) Obsolescence Risk Management Process

2.2 Life Cycle Stage

Most software and hardware pass through several life cycle stages corresponding to change which is embedded in electronic component. Fig. 1 is a representative life cycle curve and risk of units shipped per time, which depicts the six common life cycle part phases: Introduction, Growth, Maturity, Decline, Phase-out, and Obsolescence. Table I and the proceeding discussion summarizes the characteristics of the phases of the part life cycle.
A. Introduction Stage
The introduction stage in the hardware or software life cycle is usually characterized by high development costs driven by recently incurred design costs and low in embedded electronic application, frequent patches or modifications, low or unpredictable software/hardware behavior to meet electronic application requirements, and customization for suitable application. Marketing costs, at this stage, may also be high. Early OEM who use this hardware and software its introduction stage tend to value performance over price.

B. Growth Stage
The growth stage is characterized by hardware and software fulfills electronic application requirements. Increased electronic application during this stage may justify the development and use of patches or modification for better performance, which in turn improves economies of scale of performance. Mass production, mass distribution, and mass marketing often bring about price reductions. There are so many competitors in this stage since as opportunity seeking firms are attracted by the huge potential profit and strategic acquisitions; hence mergers have not yet taken place.

C. Maturity Stage
The maturity stage of the hardware and software life cycle is characterized by high-volume application which is embedded to the electronic components. Competitors with lower cost of production may enter the market, or domestic competitors may shift production facilities to cheaper locations for enabling them to the lower manufacturing costs. The inspection electronic system is an example of a mature hardware and software electronic application.

D. Decline Stage
The decline stage is indicated by decreasing demand and generally decreasing profit margin.
Towards the end of the decline stage, only a few specialized industries remain in the market. The unexpandable PLC or microcontrollers are examples of hardware and software electronic application that have been available very late due to continued electronic application in the legacy pharmaceutical equipment.

E. Phase out and Obsolescence Stage
The phase out and obsolescence stage are the final stage of life cycle whereas hardware and software which is used in electronic application has been replaced by the new hardware and software. Hardware and software use to maintain operations of legacy pharmaceutical equipment due to low utilization or complex system that impact to the business which more challenges to be upgraded or replaced. This is the stage whereas the risks have to be managed to mitigate and prevent loss that will impact to the business continuity.

2.3 Risk Management
Risk management is systematically to identify, evaluate and control potential losses to the organization that may result from things that have not happened yet.
There are four linked objectives in risk management, as follows:
2.3.1 Eliminate the risk
2.3.2 Reduce to ‘acceptable’ levels those that cannot be eliminated
2.3.3 Controls that keep them in acceptable condition
2.3.4 Transfer to some other organization.
There are two fundamental components on effective management to handle risk management process in information and information technology. An organization’s strategic deployment is the first relation of information technology in order to achieve its business goals. Information Technology (IT) projects often represent significant investments of financial and managerial resources. Shareholders’ interest in the effectiveness of such deployment should be reflected in the transparency according to the planning, management and measurement, and the way in which risks are assessed and controlled. The second component is the way in managing the risks incorporated with information assets themselves.
The complexity of the risk assessment will depend on the complexity of the organization and of the risks under review. The techniques employed to carry it out should be consistent with this complexity and the level of assurance required by the board. One of the primary functions of security risk analysis is to put this process to be more objective basis and conducted by a qualified and experienced person.
Risk management strategies are usually therefore based on an assessment of the economic benefits that the organization can derive from an investment in a particular control; in other words, for every control that the organization might implement, the calculation would be that the cost of implementation would be outweighed, preferably significantly, by the economic values that derive from, or economic losses that are avoided as a result of, its implementation. The organization should define its criteria for accepting risks (for example, it might say that it will accept any risk whose economic impact is less than the cost of controlling it) and for controlling risks (for example, it might say that any risk that has both a high likelihood and a high impact must be controlled to an identified level, or threshold).

3. Qualitative Risk Analysis
3.1 Assets within the scope
The first step is to identify all the information assets (and ‘assets’ includes information systems – refer to the information security policy for this definition) within the scope (4.2.1.a) of the ISMS and, at the same time, to document which individual and/or department ‘owns’ the asset.
3.1.1 Scope
a. Electronics Based control systems and Components
b. PLC & SCADA Software
c. Windows based line control systems

3.1.2 Asset list
Table 2. List of identified asset information corresponding to scope which is software and hardware embedded in electronic component are being used for pharmaceutical equipment.
3.1.3 Hardware and Software Vulnerabilities and Threats

Determine hardware and software vulnerabilities and threats to eliminate or minimized risk and keep them in acceptable condition. Threats is defined as support and substitution capabilities of hardware and software, whereas vulnerability is environment that may cause hardware and software malfunction. It will determine as an impact of hardware and software obsolescence. Table 3 is the threats and vulnerability level to determine impact obsolescence of each system.

<table>
<thead>
<tr>
<th>System Description</th>
<th>Threats</th>
<th>Vulnerability</th>
<th>Impact Obsolescence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computerized Maintenance Management System</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Windows XP Operating System</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Programmable Logic Control</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Building Automation System</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Supervisory, Control and Data Acquisition (SCADA) System</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Electronic Library Management System (ELiMS)</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Human Machine Interface (HMI)</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Table 3. Hardware and Software Vulnerabilities and Threats

3.1.4 Hardware and Software Business Impacts

Identify hardware and software impact to business and cost for system recovery to determine the criticality to business (table 4).

<table>
<thead>
<tr>
<th>System Description</th>
<th>Business Impact</th>
<th>System Recovery</th>
<th>Critical to business</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computerized Maintenance Management System</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Windows XP Operating System</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Programmable Logic Control</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Building Automation System</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Supervisory, Control and Data Acquisition (SCADA) System</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Electronic Library Management System (ELiMS)</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Human Machine Interface (HMI)</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>

Table 4. Hardware and Software Business Impact

3.1.5 Risk assessment

Asses the risk to have risk prioritization and mitigation plan (table 5).

<table>
<thead>
<tr>
<th>System Description</th>
<th>Impact Obsolescence</th>
<th>Critical to Business</th>
<th>Overall Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computerized Maintenance Management System</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Windows XP Operating System</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Programmable Logic Control</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Building Automation System</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Supervisory, Control and Data Acquisition (SCADA) System</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>
### Table 5. Risk Assessment Result

<table>
<thead>
<tr>
<th>Electronic Library Management System (ELiMS)</th>
<th>Low</th>
<th>Low</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Machine Interface (HMI)</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

#### 3.1.6 Risk mitigation strategy

There are four strategies to mitigate the risks which are related to compatibility, reaction time, sustainability, effort and innovation are as follows:

3.1.6.1 Last time buy
- Backup software or stock obsolescence hardware. It provides less effort and time, more compatibility. It will be used as short term solution.

3.1.6.2 Substitution
- Substitute with new hardware and software if applicable. It provides compatibility but need more time and effort. It will be used as short to medium term solution.

3.1.6.3 Re-design
- Redesign new software and hardware as per intended use. Time consuming since it develops the software and hardware form beginning. More effort and current process knowledge and experience in translating the hardware and software obsolescence to the new one. Innovation supposed to be applied to execute this solution. It will be used as medium to long solution.

3.1.6.4 Migration
- Time consuming since it has to learn old software and hardware system prior to develop the new software and hardware. More effort and current process knowledge and experience are mandatory requirement in migrating the hardware and software obsolescence. Innovation must be applied to execute this solution. It will be used as long solution.

---

**3.1.6 Risk mitigation strategy**

There are four strategies to mitigate the risks which are related to compatibility, reaction time, sustainability, effort and innovation are as follows:

3.1.6.1 Last time buy
- Backup software or stock obsolescence hardware. It provides less effort and time, more compatibility. It will be used as short term solution.

3.1.6.2 Substitution
- Substitute with new hardware and software if applicable. It provides compatibility but need more time and effort. It will be used as short to medium term solution.

3.1.6.3 Re-design
- Redesign new software and hardware as per intended use. Time consuming since it develops the software and hardware form beginning. More effort and current process knowledge and experience in translating the hardware and software obsolescence to the new one. Innovation supposed to be applied to execute this solution. It will be used as medium to long solution.

3.1.6.4 Migration
- Time consuming since it has to learn old software and hardware system prior to develop the new software and hardware. More effort and current process knowledge and experience are mandatory requirement in migrating the hardware and software obsolescence. Innovation must be applied to execute this solution. It will be used as long solution.
4. Discussion

Every factory has to submit the asset list of the manufacturing system and apply mitigation strategy as per required. Risk assessment should be applied into all assets that within the scope of hardware and software obsolescence. Determine the risk prioritization base on risk assessment to mitigate the risks and apply appropriate strategy according to business and obsolescence impact. Hence, electronic components which are used for equipment can be operated as per intended use. Apply mitigation strategy as per risk prioritization matrix as shown in table 6 below:

<table>
<thead>
<tr>
<th>Risk Prioritization</th>
<th>Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1=Last Time Buy</td>
</tr>
<tr>
<td>Low</td>
<td>🧡🧡🧡</td>
</tr>
<tr>
<td>Medium</td>
<td>🧡🧡</td>
</tr>
<tr>
<td>High</td>
<td>🧡</td>
</tr>
<tr>
<td>Critical</td>
<td>🧡</td>
</tr>
</tbody>
</table>

Table 6. Mitigation strategy base on overall risk result

5. Conclusion

Pharmaceutical industries face challenges in hardware and software obsolescence since most of these industries have been built for many years and use old technology in running their factory. The IT Risk Management is a methodology which can be used to identify, eliminate, reduce and control their hardware and software obsolescence in acceptable condition.

There are some steps in conduction the Risk Assessment of hardware and software obsolescence:

1. Identify assets within the scope
2. Determine Life Cycle
3. Identify Hardware and Software Vulnerabilities and Threats as obsolescence impact
4. Hardware and Software Business Impacts to find out the software and hardware criticality to the business.
5. Risk Assessment to assess and prioritization the risk according to the obsolescence and business impact.
6. Risk Mitigation Strategy as a mitigation plan to eliminate, reduce or maintain the hardware and software in acceptable condition.
7. Apply risk mitigation strategy based on risk prioritization.

IT Risk management of manufacturing system in pharmaceutical industry result for this paper can be found in table below:
System Description | Overall Risk | Mitigation Strategy No Primary | Mitigation Strategy No Secondary
---|---|---|---
Computerized Maintenance Management System | Low | 1, 2, or 3 | 4
Windows XP Operating System | High | 1 | 2 or 3
Programmable Logic Control | High | 1 | 2 or 3
Building Automation System | Medium | 1 and 2 | 3 or 4
Supervisory, Control and Data Acquisition (SCADA) System | Medium | 1 and 2 | 3 or 4
Electronic Library Management System (ELiMS) | Low | 1, 2, or 3 | 4
Human Machine Interface (HMI) | High | 1 | 2 or 3

1 = Last Time Buy 2 = Substitution 3 = Re-design 4 = Migration

Table 7. Risk assessment result and mitigation strategy

References: