# Process design principles in relation to risk management

**The following content assists in answering Q15 in AT1.**

This content has come from <https://www.heflo.com/blog/bpm/business-process-design-principles/> and been contextualised to suit risk management.

**Overview**

According to the above website: *“Business process design is a BPM step that occurs after the analysis and discovery steps. Its goal is to create an improved and optimized process that meets all of your expectations in relation to process performance and strategic business needs.”*

If we look at this in the context of risk management, risk management is a process we need to follow to, as the name suggests, reduce the risk for our business when a threat and vulnerability is identified. The risk management steps vary depending on where you look, however a good set of steps is:

1. Establishing the context.
2. Identifying the risks or threats.
3. Assessment of the risks.
4. Potential risk treatment.
5. Creating the plan.
6. Implementing the risk management plan.
7. Review and the evaluation of the plan.

A good definition of “process” is: *“a series of actions or steps taken in order to achieve a particular end.”* So, if we are designing a process to reduce our risk, any process would need to include the above 7 steps for it to be complete. The above steps have been or will be covered in the BSBXCS404 course. The actual process we design however need to follow certain principles in order for it to be complete and accurate, but also have people want to follow it. Below we will discuss the **design principles**, as opposed to the **process** itself.

The following principles are from the provided website (*in italics*), with additions to provide a security context (in bold).

## 1- Moments of truth

*Moments of truth in business process design concerns all the interactions between clients and the company.*

*They are the “moments of truth” because they are interactions between the organization and the customer, who is, perhaps, experiencing your services or products for the first time.*

*And why is this important?*

*This moment must be “magic”! The client should feel that their wants and needs have been fully met.*

**In the context of security, this could be interpreted as “Whatever process you design needs to solve the client’s problem”**

## 2- Adding value for the customer

*To understand this principle simply answer this question:*

*Would your customer pay for this activity?*

*We have to specify these activities because they’re the ones that will lead to the moments of truth, they’re the ones that make the product or service more valuable in the eyes of the client and must be the subject of improvement studies.*

*For activities that don’t add value, these should be eliminated in the design of the new process.*

**In the context of security, we need to be able to answer questions like “does the cost of the control match the risk?”. When designing processes, we need to take into account the full cost of the control. This could include initial purchasing costs, ongoing costs (e.g. licensing), monitoring and so on.**

## 3- The reduction of Handoff delays

*A Handoff occurs when there is an exchange of responsibility between teams. This is a critical moment.*

*Why?*

*Failures, errors and delays can occur at this time, with some risk of getting them wrong during the operation.*

*<Website data removed here>*

*Ideally you need to mitigate handoff problems as much as possible when redesigning business processes.*

*What should you do?*

*Use automation technology wisely.*

*A good workflow configuration will allow process instances to migrate from one team to another securely, bringing with it all the data that’s required for the target team to perform its intended tasks in the process.*

**In the context of security, this is particularly important where multiple teams are involved. As part of the process is handed from one team to another (such as during a problem escalation), it is important that the process is as seamless as possible. Automated systems can help in this instance. Team 1 records everything, so that when team 2 takes over, all of team 1’s notes are available.**

## 4- Caution: Avoid over-automating!

*There was a tendency, which is now outdated, to automate everything possible, indiscriminately.*

*This misconception ended up simply making an old process equally ineffective and inefficient, with the only difference to the redesigned project being: instead of people running the activities, there were automated activities.*

*Remember this:*

*Business process design aims at delivering quality, whether this is via automated processes or not.*

**This is almost the opposite in some ways to step 3 which promotes a degree of automation. When designing security controls as a risk management process, a degree of human oversight should still be engineered into the process. Some systems, such as IDS/IPS, need automation due to the data processing speeds. In the event of an issue however, a human should be brought in. Humans will also be needed to confirm the automated system is functioning as expected.**

## 5- Business process standardization

*An organization has an extensive series of processes, many of which are interconnected.*

*If these processes can be reused by the company, ie they “speak a common language”, the operation as a whole will improve, in speed and agility.*

*Here are some standardization design benefits:*

* *It facilitates the operation: standardized processes represent simpler procedures and are easy to learn and memorize. This will positively impact productivity as well as safety.*
* *Increased productivity: As the team has fewer issues and makes fewer mistakes, increased productivity is a consequence.*
* *Higher quality products and services: standardization is perceived by your customers, who use it to form a concept of quality regarding your business.*
* *Reduced costs: less staff time, less resources = cost rationalization.*

**When designing risk management processes, standardising the process is important. It means that everyone knows the way things need to be done, all templates are the same, the document control system matches for every document created, and so on. Standardising processes creates higher quality output.**

## 6- Business rules

*There are some rules that must permeate the operation and the processes, facilitating their execution and, mainly, decision making.*

*<Content modified from the website>*

*Maintaining documented and up to date rules can be very difficult. So during the process design phase it’s very important that rules are identified, listed, documented, and kept consistent.*

*In addition, business rules are very volatile and change constantly and for that reason they should be periodically reviewed.*

**In the context of risk management, you need to consider business rules such as:**

* **Codes of ethics**
* **Company policies**
* **Strategic plans**
* **And so on**

**Any risk management plan you create needs to conform to business rules/documents, or else the documents need to be updates to comply with the risk management strategy being put in place.**

# 7- Compliance

*Apply the most commonly used standards for the market segment to which your company belongs.*

*Remember to check if there is a national standard that may be different from the international standard and which one is best to use.*

*An example of compliance affecting many organizations is Sarbanes Oxley, which regulates publicly traded companies in the United States.*

**ICT has what could be seen as an advantage or a disadvantage: there are standards for EVERYTHING. For example, we have Australian Standards (AS), International Standards (ISO), as well as legal requirements (Australian privacy laws). Whatever process design you come up with at a minimum should meet legal requirements, but also the standards should be consulted, as these are often seen as “best practice”.**

## 8- Validating the business process design

*It’s very important that the people working in the process are part of every phase of a BPM implementation, and business process design isn’t any different.*

*Well … the most discussed form in the CBOK for validation is process simulation, but I believe the best way to validate a process is by submitting a prototype for the evaluation of those people who perform in the execution of the process.*

*<Website content removed, but worth reading>*

**When designing a process for risk management, this principle relates to the testing of the process. A common testing method could be prototyping. If you design the process in such a way that it can be tested at small scale, you can confirm it works before scaling it to full size.**

## 9- Simplicity in business process design

*Whenever we look for the* ***complete*** *solution, we fall into the mistake of the* ***complex*** *solution.*

*Complexity will not bring any benefit to the design of your process. Definitely!*

*A complex process or operation results in unnecessary expenses, errors, low productivity and delays. We usually call this “bureaucracy” (read “excess bureaucracy”).*

*Actually a good design job is one that after hours and hours of work results in something simple, containing only the essence necessary to make the process capable of achieving the expected performance.*

**In our context, this would be interpreted as “So long as it solves the problem, simpler is better”. Each extra step in a security process is an additional point of failure. If you are able to keep processes relatively simple, they are more likely to be followed, are easier to monitor, and easier to implement.**