Continuous Auditing

Continue in control met Continuous Auditing.
Door Bart de Best

Context:
This story is based on an assignment from a temporary employment agency to provide a high frequency of control monitoring of internal and external requirements such as privacy, security and legislation and regulations.

Challenge:
The challenge of this assignment was that it was only with difficulty that it was difficult to demonstrate that IT service provision was in order at an annual level through manual evidence. Controls were often not defined, and evidence was lacking. There was no large budget to make a radical improvement. All improvements had to be designed incrementally and iteratively after approval.

Solution:
The solution for this assignment was found in the concept of Continuous Auditing. This blog discusses how Continuous Auditing has been applied using the following steps:

1. Determine the controls
2. Determine the design criteria
3. Determine the evidence
4. Determine the evidence collector
5. Determine the continuous auditing engine
6. Determine the dashboard

The total solution is shown in figure 1. Steps 1 to 6 were first completed manually. Then, based on the frequency of the controls and the time required to measure them, it is determined how the monitoring of the control can be digitized.

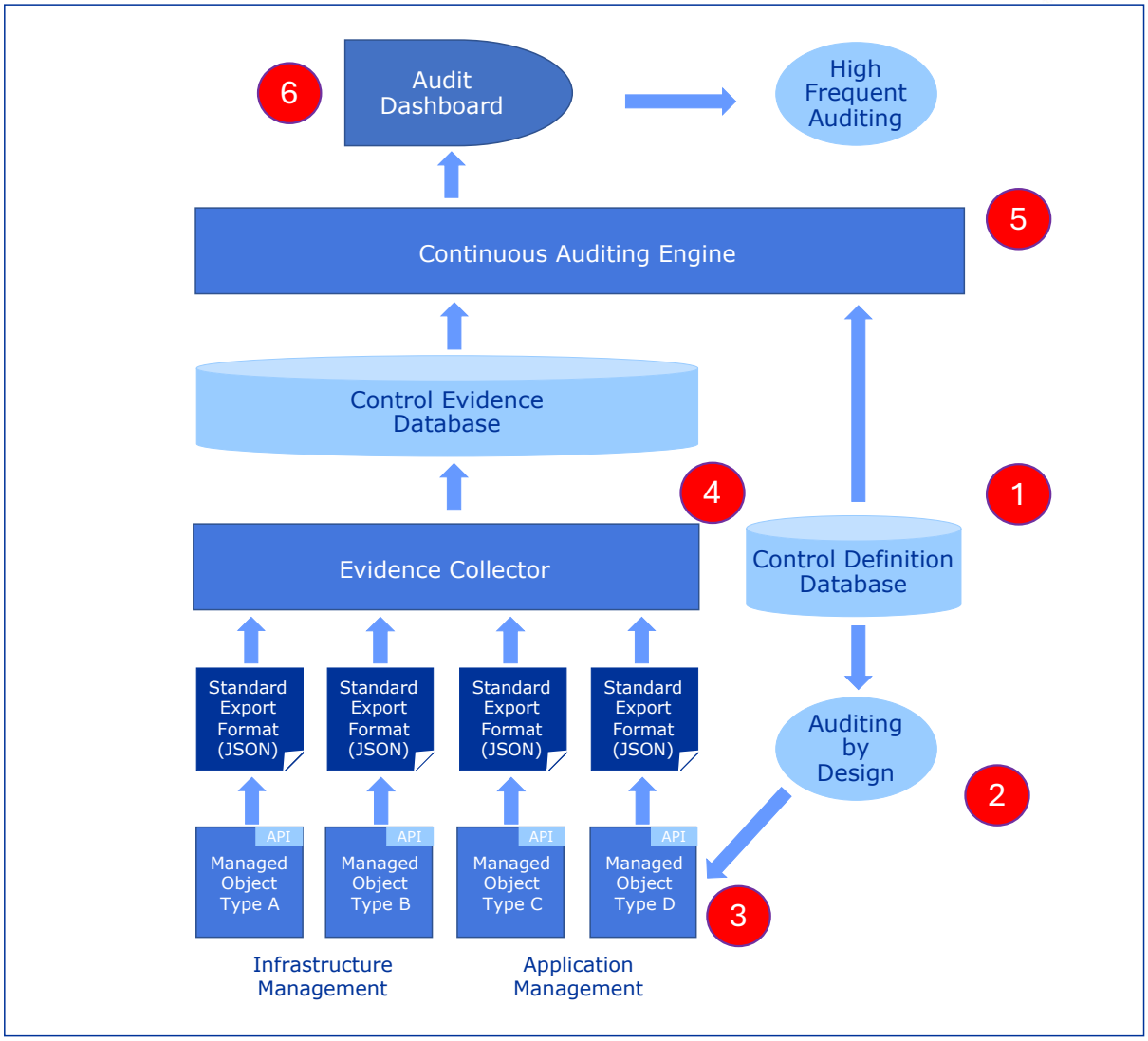


Figure 1, Continuous Auditing concept.

1. Determine the controls

The control definition database is the core of this audit approach. Controls are the countermeasures to the risks that need to be managed. The risks have been obtained from various sources such as:

- Ricks from business goals
- Risks of business value stream goals
- Risks from audits
- Risks from legislation & regulations
- Risks from standard frameworks such as ISO 27001
- Risks from change management and service level management

The countermeasures are assigned based on the classification of the risks, namely:

- Modify: come up with a countermeasure (elimination or mitigation risk)
- Avoid: consider how the risk can be avoided (e.g. notebook only in the office)
- Share: share the risks (e.g. taking out insurance)
- Retain: take the risk (no action required)

Only the risks that need to be controlled (modify) are provided with a counter-measure. The information footprint has also been determined for the controls, which makes it possible to determine whether the countermeasure is effective. Finally, the frequency of the measurement is recorded in the control. ISO 27001 has proven to be the most important source of controls.

2. Determine the design criteria

The design criteria concern both the design and the design requirements that ensure that the countermeasure is effective and measurable. These design criteria are included in the acceptance criteria of the product backlog items. An example is the scalability of an infrastructure facility so that peak loads do not disrupt the accessibility of information. Another example is to ensure the confidentiality of data by introducing two-factor authentication.

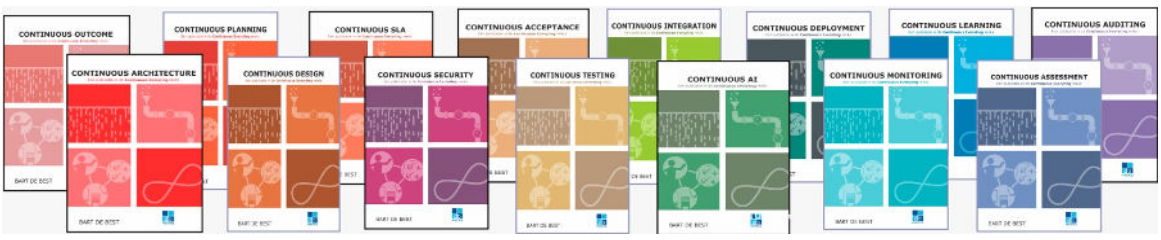
3. Determine the evidence

Based on the control definition, it is determined which objects to be managed (managed objects) are in scope for risk management. This was done by drawing up a portfolio of application services and infrastructure services and then determining which controls are important for each item. The number of controls per item appeared to be manageable.

It is then determined how the information footprint, as defined in the control, can be extracted from the managed object and in what format this can be done. This is not always possible with a REST API, but it has proven possible to extract the information from the object. This interface can be built using a microservice. An example is reading a firewall to determine whether ports are wrongly open. Or reading an application to determine whether it contains suspicious transactions.

4. Determine the evidence collector

The evidence collector periodically retrieves the evidence from the managed objects. Instead of a pull mechanism, a push mechanism is of course also possible. As long as the frequency of evidence collection is in accordance with the controls. In the short term, a manual collector was chosen based on different collection frequencies defined in the controls.



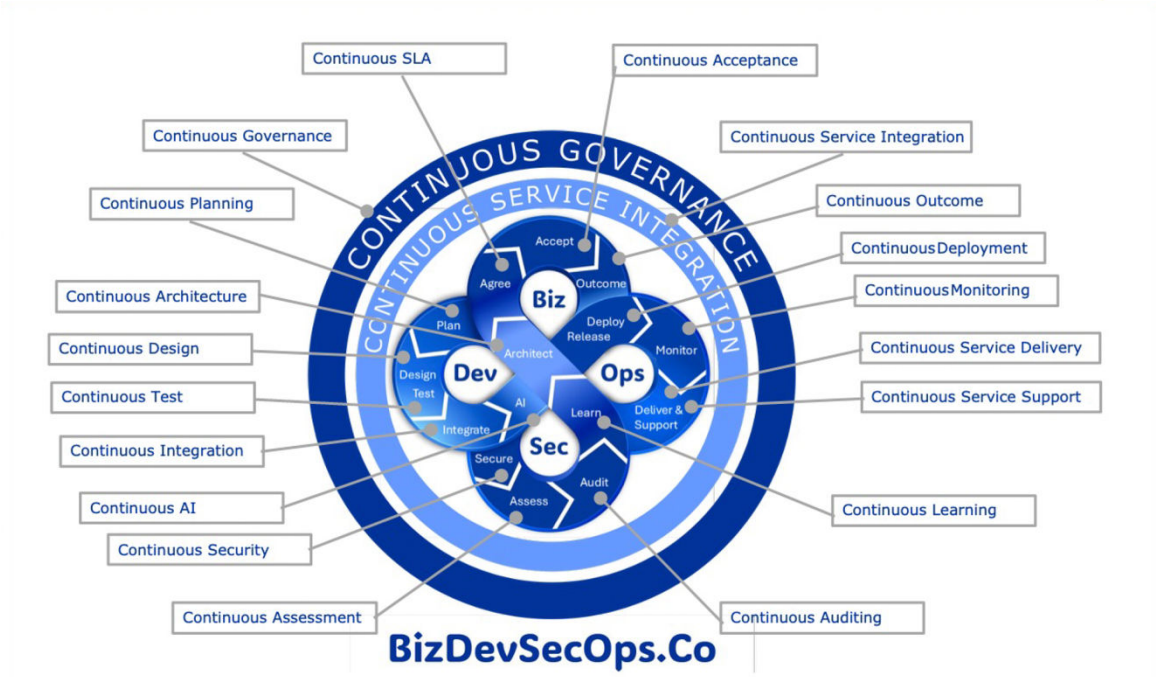
5. Determine the continuous auditing engine

The audit engine is a simple step. Only a verification needs to be carried out between the control definition and the collected evidence. This step was also first performed manually to determine that the logic worked correctly.

6. Determine the dashboard

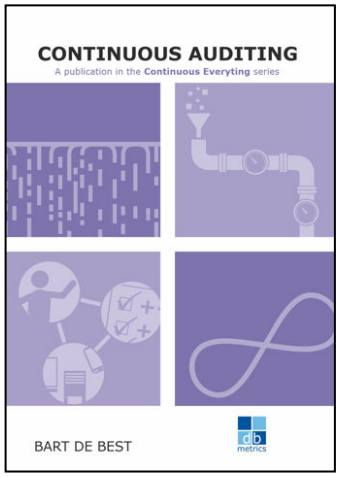
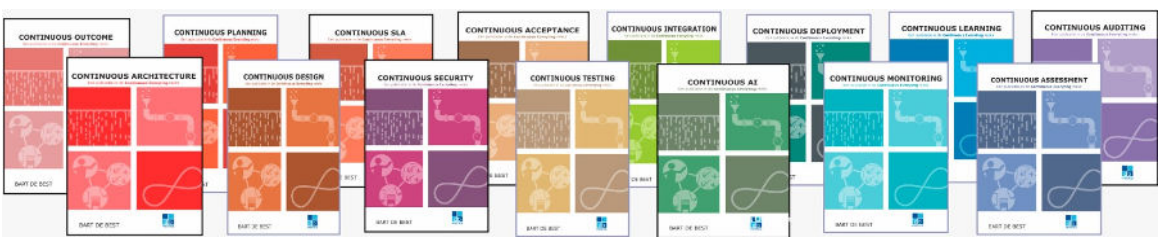
The dashboard provides reporting on the results. The periodicity is determined by the controls. Because the first step was carried out manually, the frequency of publication on the dashboard also had to be kept low. With each step of digitalization, the frequency per control has increased.

This simple approach of continuously measuring being in control is very attractive because the degree of control is continuously determined. This form of auditing is therefore a good example of Continuous Auditing.



Interested in a demo voucher or learning more about the BizDevSecOps Assessment? Please contact us at:info@bizdevsecops.co

For more details about the assessment, please click here:LINK



Author: Bart de Best
Website: www.*BizDevSecOps.Co*
Email: info@bizdevsecops.co
For more details about publication, please click here: LINK