The "Self-Assessment" Method within a Mature Third-Party Risk Management Process in the Context of Information Security

Proceedings of the 2021 International Conference on Information Technologies (InfoTech-2021), IEEE Conference, Rec # 52438

Veselin Monev, PhD

Information Security Professional

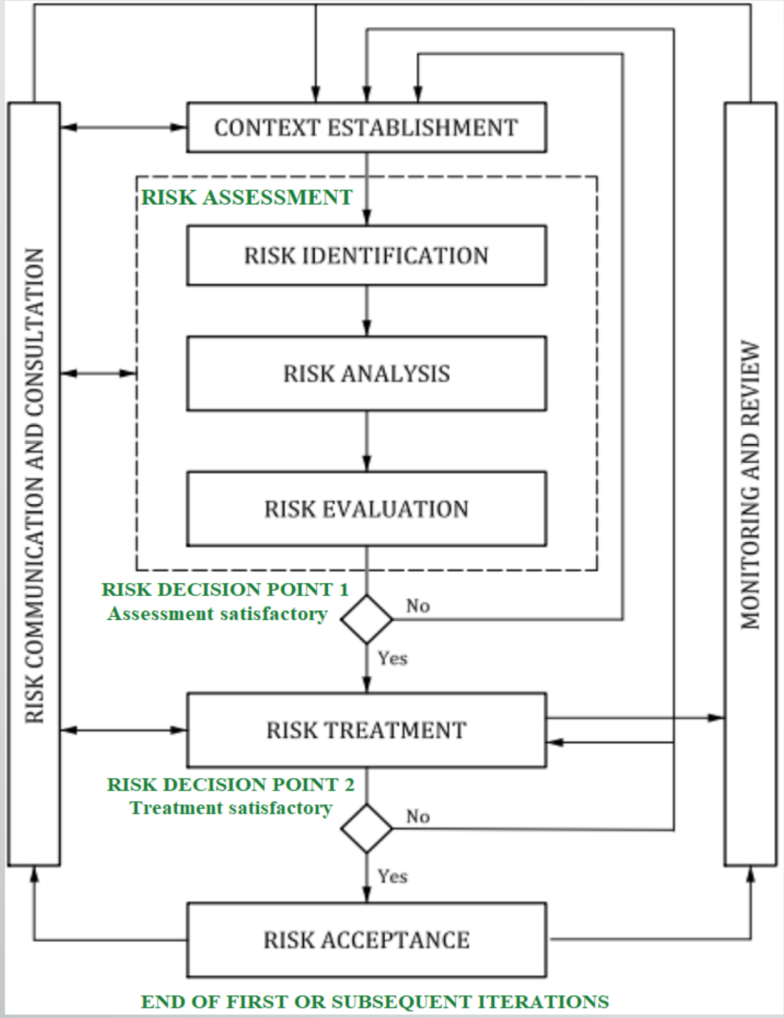
September 2021

Problem:

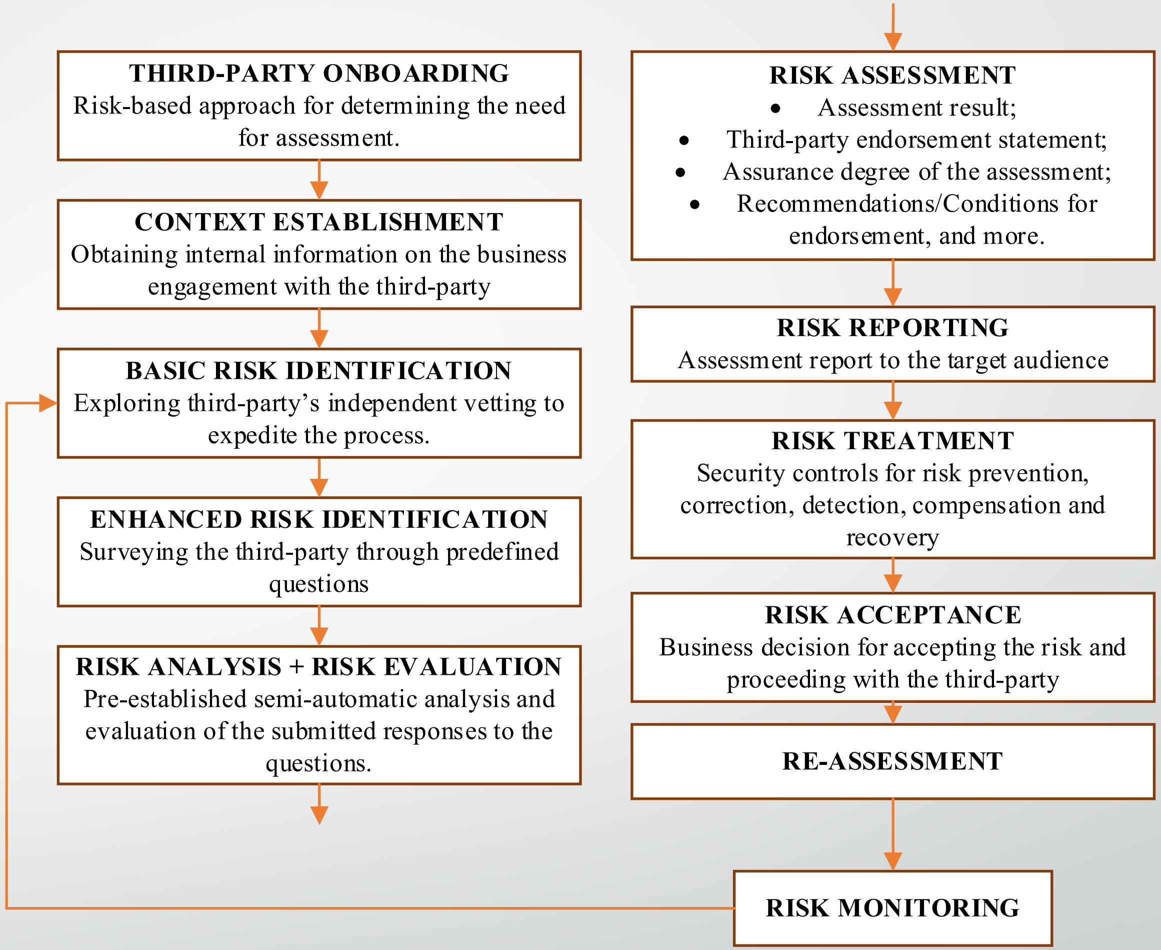
- Third-party risk assessment/management programmes in organisations are immature.
- Current software solutions use <u>surveys</u> with automatic scoring capabilities that are not aligned with established information security risk assessment practices, such as ISO 27005 or NIST 800-30.
- There is a need for the execution of proper periodic information security risk assessments instead of surveys with automatic scoring.

Solution:

- A third-party risk management process that aligns closely with ISO 27005.
- Vendors of software solutions for risk management through surveys and their customers can modify the software solutions in alignment with the process.



ISO 27005:2018; Information Security Risk Management Process (original colors modified)



THIRD-PARTY ONBOARDING
Risk-based approach for determining the need for assessment.

CONTEXT ESTABLISHMENT
Obtaining internal information on the business engagement with the third-party

BASIC RISK IDENTIFICATION
Exploring third-party's independent vetting to expedite the process.

ENHANCED RISK IDENTIFICATION
Surveying the third-party through predefined questions

RISK ANALYSIS + RISK EVALUATION
Pre-established semi-automatic analysis and evaluation of the submitted responses to the questions.

RISK ASSESSMENT

- Assessment result;
- Third-party endorsement statement;
- Assurance degree of the assessment;
- Recommendations/Conditions for endorsement, and more.

RISK REPORTING
Assessment report to the target audience

RISK TREATMENT
Security controls for risk prevention, correction, detection, compensation and recovery

RISK ACCEPTANCE
Business decision for accepting the risk and proceeding with the third-party

RE-ASSESSMENT

RISK MONITORING

Proposed Third-Party Risk Management Process

Process benefits:

- Innovating third-party risk management.
- Very close alignment with ISO 27005.
- Increased value of the assessment results for business-decision makers.

Process downsides:

- Challenging to implement in organizations with low risk culture and maturity.
- Semi-automated workflow requires competent security professionals to operate the process.