

# Automatic Verification and Diagnosis of Security Risk Assessments in Business Process Models (Summary)\*

Ángel Jesús Varela-Vaca<sup>1</sup>, Luisa Parody<sup>2</sup>, Rafael M. Gasca<sup>1</sup>, and María Teresa Gómez-López<sup>1</sup>

<sup>1</sup> Universidad de Sevilla, Sevilla, Spain

{ajvarela, gasca, maytegomez}@us.es

<sup>2</sup> Universidad Loyola Andaluca, Sevilla, Spain

mlparody@uloyola.es

## Summary of the contribution

Organizations execute daily activities to meet their objectives. The performance of these activities can be fundamental for achieving a business objective, but they also imply the assumption of certain security risks that might go against a company's security policies. A risk may be defined as the effects of uncertainty on the achievement of the goals of a company, some of which can be associated with security aspects (e.g., data corruption or data leakage). The execution of the activities can be choreographed using business processes models, in which the risk of the entire business process model derives from a combination of the single activity risks (executed in an isolated manner). In this paper, the problem of automatic security risk management in the current BPMS is addressed. First, a formalization of the risk elements according to process models is included. These elements are supported as a BPMN 2.0 extension of risk information that is analyzed to determine nonconformance regarding risk goals. In addition, a diagnosis of the risk associated with the activity responsible for the nonconformance is also carried out. To this end, the proposal applies mechanisms based on the model-based diagnosis in which activities are in nonconformance with regard to the acceptable level of risk. The automation of diagnosis is carried out using artificial intelligence techniques based on constraint programming. The proposal is supported by the implementation of a plug-in that enables the graphical specification of the extension and the automation of the verification and diagnosis process. To the best of our knowledge, this is the first published work that addresses the risk-aware design of business processes with automatic techniques.

## Acknowledge

This work has been partially funded by the Ministry of Science and Technology of Spain (RTI2018-094283-B-C33) and the European Regional Development Fund (ERDF/FEDER).

\* This work has been published in IEEE Access, vol. 7, pp. 26448-26465, 2019. 2017 JCR Impact Factor: 3.557. doi: 10.1109/ACCESS.2019.2901408.