

Extending ISO/IEC 27005 for AI-Enabled DAOs with Risk Scenarios for Decentralized Governance and Autonomous Agents

Vincent Lalanne¹, Manuel Munier¹, Akram Hakiri¹, Laurent Gallon¹, and Richard Chbeir¹

University of Pau and Pays de l'Adour, E2S, UPPA, LIUPPA, College STEE, Anglet
`firstname(dot)lastname(at)univ-pau.fr`

Abstract. Decentralized autonomous organizations (DAOs) increasingly combine smart contracts and token-based governance with large language models (LLMs), retrieval services and tool-using agents. These integrations create socio-technical risks, because AI-generated outputs can influence collective decisions, external services can acquire de facto authority, and control can remain concentrated despite decentralized governance. This paper develops a design-oriented operationalization of ISO/IEC 27005 scenario analysis for AI-enabled DAOs. It adds four scenario fields, namely trust boundaries, practical decision and control rights, AI roles, and event or drift status with monitoring indicators, and it distinguishes asset custodians, technical control operators, risk decision authorities and independent verifiers. A qualitative prioritization rule avoids treating ordinal ratings as measurements. The approach is applied to a healthcare DAO that allocates biomedical research funding and governs access to sensitive health data through AI-assisted decisions. Six analytically derived risk families become scenarios with explicit paths, decisive vulnerabilities, treatment responsibilities and residual-risk decisions, and a self-assessment identifies gaps and limits. The artefacts give a traceable basis for later empirical evaluation, without implying validated effectiveness in operational DAOs.

Keywords: Decentralized autonomous organizations · AI security · ISO/IEC 27005 · smart contracts · governance attacks · risk scenarios · autonomous agents

1 Introduction

Decentralized autonomous organizations (DAOs) coordinate shared resources through smart contracts, token-based voting, blockchain records and off-chain social and technical processes [1]. Although they are designed to distribute decision-making authority, practical control may remain concentrated among developers, delegates, multisignature signers, oracle operators, infrastructure providers or a few highly active voters [3]. Artificial intelligence (AI), and large language models (LLMs) in particular, increasingly supports proposal summarization, evidence retrieval, risk assessment, code generation and interaction with