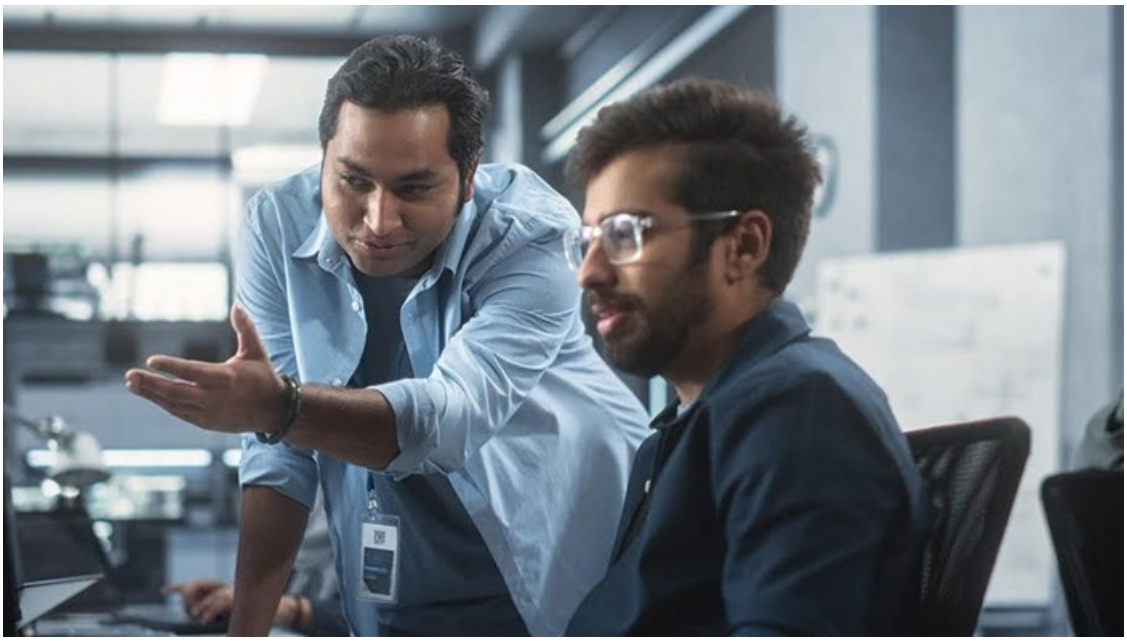
BIZCOMMUNITY

Why software escrow gives SA fintech developers the edge

Issued by Escrowsure

26 Feb 2024

In large corporations, digital transformation is impacting every customer touchpoint, yet this rapid innovation for operational advancement could be what exposes them to operational risk. The uptake of bespoke third-party software solutions is essential to enable financial services and insurance companies to meet the demands of their daily business operations. But what happens if your third-party software vendor goes out of business or is unable to maintain services?



Software escrow is internationally accepted as best practice to manage the risks associated with exposure from third-party software providers. It is a customised legal agreement between the software developer, the user, and the software escrow agent. This safeguards the software source code and makes it available to the user in the case of clearly defined trigger events that threaten business continuity. Typically, the corporate entities bear the burden of addressing software dependencies and mitigating the risks to business continuity. However, Guy Krige, executive risk consultant at Escrowsure argues that software developers and start-ups also have a critical role to play. In a highly competitive arena, fintech start-ups that include software escrow in their go-to-market strategies show their commitment to safeguarding their clients' digital futures and gain the upper hand over competitors.

Krige says, "Software developers entering into software escrow agreements offer a proactive solution to the risks associated with service disruptions. These agreements act as a safeguard against unforeseen circumstances such as vendor insolvency, acquisition, or the inability to maintain services. For start-ups competing for sales ascendency and funding, building resilience into software solutions becomes a key differentiator. By proactively embracing escrow agreements and ensuring compliance with evolving regulations, these software vendors not only enhance their value proposition but also gain a competitive edge when vying for new clients." For 20 years, Escrowsure has been trusted by some of the world's central banks, South Africa's leading financial services and blue-chip corporates to mitigate software risk through flexible escrow solutions customised and specific to each unique business risk environment.

Riding the waves of global and local regulatory changes

As the risks associated with increasing reliance on third-party software vendors reverberate across all sectors of business, there have been successive waves of new digital risk rules and regulations aiming at conserving business continuity and

consumer protection. South African software developers and start-ups planning to gain local and global clients must be able to navigate and comply with regulations such as:

- The South African Financial Sector Conduct Authority & Prudential Authority which includes the **Joint Standard** setting out the principles for IT governance and risk management that financial institutions must comply with, in line with sound practices and processes in managing IT risk.

- The European Union's ***Digital Operational Resilience Act (DORA)*** which imposes updated cyber security and resilience requirements on European financial institutions and their critical suppliers.

- The UK's ***Prudential Regulation Authority (PRA) SS2/21*** which urges UK institutions to review third-party arrangements and evaluate the need for software escrow. The UK's ***National Risk Register 2023*** also identified technological failure on the part of suppliers as a potential risk facing UK businesses and consumers.

- The USA's Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC) and Federal Reserve Board's (FED) joint statement on outsourcing and third-party risk management for banking institutions, which highlights software escrow as an important consideration.

- The Reserve Bank of India's (RBI) ***draft Master Direction*** which includes controls that must be deployed and complied with by April 2024, and specifies the requirement that the source code of critical applications must be acquired, and if that is not possible, the RBI expects institutions to take up software escrow or a similar solution.

- ISO 27001:2022 which already requires that 'source code of the software is protected by escrow agreements' for outsourced developments.

Many of these guidelines and regulations are expected to recommend software escrow as effective third-party risk management and vital components of business continuity plans.

Andre Symes, group chief executive officer at Genasys Technologies, a technology provider servicing the insurance industry says, "Our policy and claims administration software forms the backbone of our clients' insurance operations. It is essential to the daily operations of our regulated clients and to ensure that claims get paid to the policy holders. As such having our software in escrow is not optional, but rather a necessity. Having a trustworthy escrow partner is no longer optional in today's digital age."

Krige says, "It is clear which way the wind is blowing, and in 2024 and beyond, we anticipate the ongoing introduction of additional regulations aiming to ensure businesses and consumers are protected from unexpected disruptions. It's surely time for software developers and FinTech start-ups to have their finger on the pulse and to integrate software escrow into their business models."