

CGF

RESEARCH INSTITUTE
(PTY) LTD

Professional Active Escrow

(This is an abridged version of the full report which is available for purchase. The 41 page report may be used throughout your company.)

“Our deepest fear is not that we are inadequate. Our deepest fear is that we are powerful beyond measure. As we are liberated from our own fear, our presence automatically liberates others.”

Nelson Mandela



CGF Research Institute (Pty) Ltd
Reg. No. 2004/000744/07
+ 27 11 476 8264 / 1 / 0
+ 27 82 373 2249
www.cgf.co.za www.corporate-governance.co.za
gmeyer@cgf.co.za

INDEX

Section One

- Executive summary

Section Two

- Professional Active Escrow
 - Defining escrow & its purpose
 - Qualities of an escrow agent & their role
 - Containing the operational risk
 - A typical escrow arrangement & requirements
 - What is put into escrow & agreements?
 - Verification of deposits & escrow benefits
 - Testing the organization's state of readiness

Section Three

- About Escrow Europe (Pty) Ltd



Executive summary

Professional Active Escrow

(This is an abridged version of the full report which is available for internal use within your company.)

“Today, company secretaries and compliance officers all need to be able to 'tick off' good governance, as well as contain basic risk exposure such as reliance on the use of intellectual property that they do not own.”

Steve Symes (MD) - Genasys, South Africa-MD

What is software escrow?

- Software escrow is an agreement whereby a software supplier & its end-user agree that the supplier will deposit the source code & related materials of a licensed software product on behalf of an end-user (s) with a trusted 3rd party
 - the undertaking is agreed in order to warrant end-user access to that information in case the supplier, for one reason or another, is no longer able or willing to provide maintenance for the software product
 - access to the deposit of source code is for the purposes of end-user business continuity only
 - ❖ access to the deposit of source code is not intended to interfere in any way with the supplier's rights of intellectual property ownership
- Professional software escrow;
 - is a specialised legal, technical & administrative measure to safeguard the continuity of mission critical ICT applications “at arms length” from a software supplier
 - reinforces the rights of the supplier and/or developer & the end-user
 - is not simply a deposit of the source code

Why is software escrow necessary?

1. Organizations that acquire non standard, customized and / or proprietary software products purchase a license for use of such software
 - the license purchased by the organization allows it the right to use the software, **not own it**
2. An organization who purchases such a license only receives a "compiled" version of the software & the machine code for the computer to operate with
 - the original programming sources & documentation is needed if the organization wants to maintain, correct, modify and/or extend the software
3. Whilst the software source code & documentation would, without software escrow intervention, remain with supplier, the organization will usually have a maintenance agreement with the supplier
 - through the maintenance agreement, the supplier is obliged to adjust & extend the software in order to accommodate the continuously changing business needs of the organization
4. What would be the position of the organization in the event that it experiences problems with the software & the supplier cannot or will not meet its maintenance obligations any longer?
 - a. on such occasions, the organization & the supplier agree that access to the relevant material (source code & technical documentation) be given to the organization via an escrow deposit of those materials
 - b. through a contractual agreement, deposits must be verified & administered by a professional escrow agent
 - c. the agent will be entitled to release the materials to the organization in the circumstances specified in the agreement
 - d. upon release of the materials, end-user is able either to continue the maintenance of the software himself, or to outsource the maintenance to a third party

International standards for Information & Communication Technology (ICT) governance requires *organizations to establish source code escrow*

International ISO9001 guidelines for ICT good governance (ref: Escrow guide / software)

- “Source Code Escrow agreements must be set up for each software product that an organization uses. The following exceptions may be considered;
 - a. software has no business-critical functions
 - b. a software licence fee less than 3000 Euro
 - c. less than three regular users
 - d. shrink-wrapped commodity, off-the-shelf alternative products.”

Sarbanes-Oxley calls for;

- An “operational system of internal controls over financial reporting”
 - this includes;
 - ❖ all “material events” that affect business
 - this encompasses;
 - ❖ contracts for mission-critical software & their susceptibility to changes in vendor business conditions

Professional escrow is a highly effective, low cost measure to mitigate against ICT operational risk

What is an escrow agent?

- An escrow agent is a trusted, independent 3rd party with no ties or relationships to hardware or software companies which assists organizations safeguard the continuity of their business

Qualities of a good escrow agent

- Escrow agents should;
 - be independent & act as a third party separate from the primary engaging parties
 - safeguard the interests of all parties involved
 - be legally & technically & administratively competent
 - preferably have good international representation
 - offer organizations a combination of corporate legal expertise as well as technical know-how through specialist teams that comprise lawyers, consultants & ICT experts
 - follow market developments closely in order to offer organizations a solid, meaningful service
 - be able to prove their business, legal & technical credentials

The early days of escrow was nothing more than lip-service with *little, if any, assurances or solid guarantees . . .*

- Traditional software escrow was introduced approximately 20 years ago in the USA
- In the past, a software escrow merely amounted to the physical storage of the software source code in a vault by a trusted third party i.e. **passive escrow**
 - most escrow arrangements were passive in their approach & the custodians of the source code (“deposit”) were essentially banks, notaries, legal firms
 - the custodians physically 'held' a copy of the software source code as a deposit, however they did not verify whether the material deposits was;
 - ❖ technically 'correct' or an 'up-to-date' release version, or
 - ❖ that the material on deposit was complete in terms of the purpose intended
 - passive escrow is usually untested & deposits are often unusable when called upon to deliver what they promise which impacts the continuity of an organization
- Today, the approach to escrow needs to fully embrace all the business & operational risks which is dependant on intellectual material that is not owned by an organization & whose systems are reliant on such material i.e. **active escrow**
 - the aim is that the source code remains available even if the supplier no longer exists

Experience has shown that only 1 out of 10 technically unverified deposits can be deployed for immediate use. i.e. 90% of unverified deposits are not usable

... today, organizations must ensure they *contain their basic risk exposure* - this also applies to their reliance on the use of intellectual property which they do not own

- Whilst organizations depend on a licensed business application to drive their core business systems (e.g. software, hardware products) which they do not own, they effectively outsource the associated core function
 - outsourcing an organization's core or mission business critical functions implies far greater operational risk with impacts on the organization's business continuity
- Most organizations are dependant on licensed software that support their core, mission business critical systems (e.g. software names that qualify here.....SAP, BARN, JD Edwards, Oracle)
- Organizations consider software security & continuity as a critical issue within their Business Continuity strategy & plan
 - the associated Business Continuity risks must be considered in the event that such licensed software should be disrupted and / or even lost
- Organizations obtain great comfort where suppliers of business applications offer extensive measures to support critical business systems within those organizations making use of the supplier's applications

Active escrow is not a nice-to-have, it's a business necessity

Company executives must vigilantly guard against possible operational risks related to 3rd party software systems being used within their organizations . . .

- Amongst other, 3rd party software can dramatically increase the operational risk within an organization if it is not managed correctly
 - mismanaged 3rd party software can seriously compromise the business continuity of that organization resulting in serious repercussions for the organization & its executives in their personal capacities (Companies Act, Section 424)
- Many organization's core, mission-critical systems is dependent on software which is licensed from 3rd parties rather than owned in-house
 - accordingly, such mission-critical systems is subject to conditions or events beyond the licensees' (organization's) control e. g. unforeseen developments on the part of the supplier, namely; change of ownership or strategic priority
- Whilst many organizations may utilize software escrow & assume the deposit to be complete & deployable, research shows that 90% of source code held in passive escrow deposits are useless because the deposit is not verified by technical specialists*
 - traditional software escrow does not provide for a business's continuity should its software partner no longer be in a position to continue maintaining & supporting the systems it has provided

Mismanaged 3rd party software used in an organization can inadvertently expose it to high levels of operational risk

* Ref: Three questions for CEOs about third-party software programs & how these could raise operational risk

Most corporate governance guidelines, protocols & imperatives hold *directors personally responsible* to protect the organization's assets . . .

- Corporate governance guidelines, protocols & imperatives such as Basel II, King II, COSO II, Turnbull, Sarbanes Oxley & ISO 17799 insist that company directors ensure that;
 - procedures & practices are in place to protect the organization's assets & reputation
 - the organization complies with all laws, regulations & best business practice
 - technology & systems in the organization are adequate to run the organization properly
 - ICT & software risks are identified & addressed
- The Turnbull Report (UK) effectively envisages a risk management program which undertakes the following key tasks;
 - identifies the nature & extent of risks facing the organization
 - prioritizes the risks
 - implements control procedures
 - monitors ongoing processes

“...it is important that the boards of directors of all companies take a robust approach to risk management & particularly in relation to IT-related risks.”

Turnbull Report

Increasingly, organizations depend on their suppliers to provide support & maintenance of their applications - a practice considered fatal should things go wrong . . .

Technology users / beneficiaries of an escrow contract

- There is significant risk exposure to companies that rely on their suppliers to provide support & maintenance of its applications, particularly where business critical applications are concerned
 - where a company itself cannot contain its risk, it should consider using a trusted independent third party to assist identify, mitigate & eliminate various risk exposures through an escrow agreement
 - potential risks a company should consider, include;
 - ❖ supplier's inability/failure to fulfill maintenance commitments
 - ❖ collapse of the supplier providing business applications
 - ❖ supplier insolvency
 - ❖ mergers & acquisitions
 - ❖ redundant technology
 - ❖ accounting scandals

If you use software & applications for important business processes, then security & continuity are of prime importance, even if the supplier is no longer able to fulfill his obligations

... organizations should draw advice from professional advisors as an additional precaution when entering & maintaining contracts that support business critical applications

Professional advisors

- Notaries, company lawyers, accountants or strategic buyers are generally individuals responsible for protecting the legal and/or economic interests of an organization
 - these individuals should have the necessary experience & capability, either in their individual and / or joint capacities to combine legal know-how with technical expertise
 - where such skills may be lacking, organizations should expect to draw advice & experience from their professional escrow agents
 - organizations need to be assured their business is safe-guarded; in particular;
 - ❖ deposits must be verified for its legal & technical integrity before they are deposited & stored in a secure safe
 - ❖ the verification must be performed impartially
 - ❖ the parties verifying the deposit must provide detailed status reports to the supplier & their clients providing variances, if any, from agreed contracts
 - ❖ deposits must be updated on each occasion where necessary & tested
 - ❖ up-dated deposits must be regularly checked to ensure they correspond with the applications being used by the clients
 - ❖ modifications to relevant & implicated contracts also need to be considered

How to order this report

Report name: Professional Active Escrow

Pages: 41

Reviewers: CGF Research Institute (Pty) Limited ("CGF") would like to express its appreciation for the peer review & editorial contribution to this presentation by Andrew Stekhoven (MD: Escrow Europe (Pty) Ltd).

Price: R 580.00 ex Vat

Price: R 661.00 incl Vat

Should you wish to order this report, please supply CGF Research Institute (Pty) Ltd the following information:

- 1) Your company's name (in full) to be invoiced;
- 2) Your company's registration number;
- 3) Your company's VAT registration number;
- 4) Your company's physical address;
- 5) Your company's postal address;
- 6) The person's name who will be taking delivery of the product; designation and email address.

Submit your information to: accounts@cgf.co.za

Our process from here:

- 1) On receipt of the above information;
- 2) An invoice will be issued with our terms and conditions ("t's&c's") attached;
- 3) On receipt of the signed t's&c's and proof of payment, we will send the report electronically to your designated email address.

Banking details:

Bank: First National Bank

Branch: Cresta Centre

Branch Code: 254-905

Account Number: 6-206-290-027-2

Account Holder: CGF Research Institute (Pty) Ltd

More information about CGF: www.cgf.co.za or www.corporate-governance.co.za