



SOURCE CODE ESCROW VERIFICATION

**An Often Overlooked Crucial
Component of BCP**

Who is APPS Global?

Specialist business with focus on

- Source code verification
- IP Asset Management
- Source Code Escrow

Business Continuity

- Disaster tolerance in business
- Risk management
- Organisation Wide
 - Buildings and Facilities
 - Personnel
 - Operating Procedure / Governance
 - IT Systems

Software Escrow

- Holding of software on behalf of two contracting entities by a trusted third party
- In practice, deposit and forget
- How confident are you that escrow has addressed your risks?
 - 80%, 90% 100% ??

Escrow is an essential first step towards ensuring support for business continuity .. but

The Catch?

Software escrow itself has significant risks...

to remain effective, it requires ongoing management and maintenance.

REALITY CHECK

***AN ESTIMATED 80% OF SOURCE
CODE ESCROW WILL FAIL
COMPLETELY***

THE SOLUTION?

ONGOING

SOURCE CODE

VERIFICATION

Common Escrow Problems

- System deposit was incomplete
- System had many dependencies
 - Hardware and Software
 - Changed over time
- Key documentation was missing
- Patches and customisations were lost

Software Escrow Risks

- Delay in initial escrow deposit
- Critical information missing
 - System rebuild steps
 - Specification and design documents
- Dependent software
 - Software Development Tools
 - Operating system libraries eg. Drivers
 - Databases
- Operating System Maintenance
 - Bug fixes, patch sets

Software Escrow Risks

- Operating System obsolescence
- Application obsolescence
- Customisations to the application
- Application maintenance (patches)

Software Escrow Risks

- Hardware obsolescence
- Degradation of storage media
- Virus infection

AND DON'T FORGET...

- Risk of supplier insolvency
- Cessation of product support
- Other issues resulting in non support

Escrow Risk Mitigation

- **REGULAR CONTENT VERIFICATION**
- Improve deposit preparation
- Track system dependencies
- Regular media refresh
- Comprehensive escrow management
- Maintenance levels matched to risk

Verification Approach

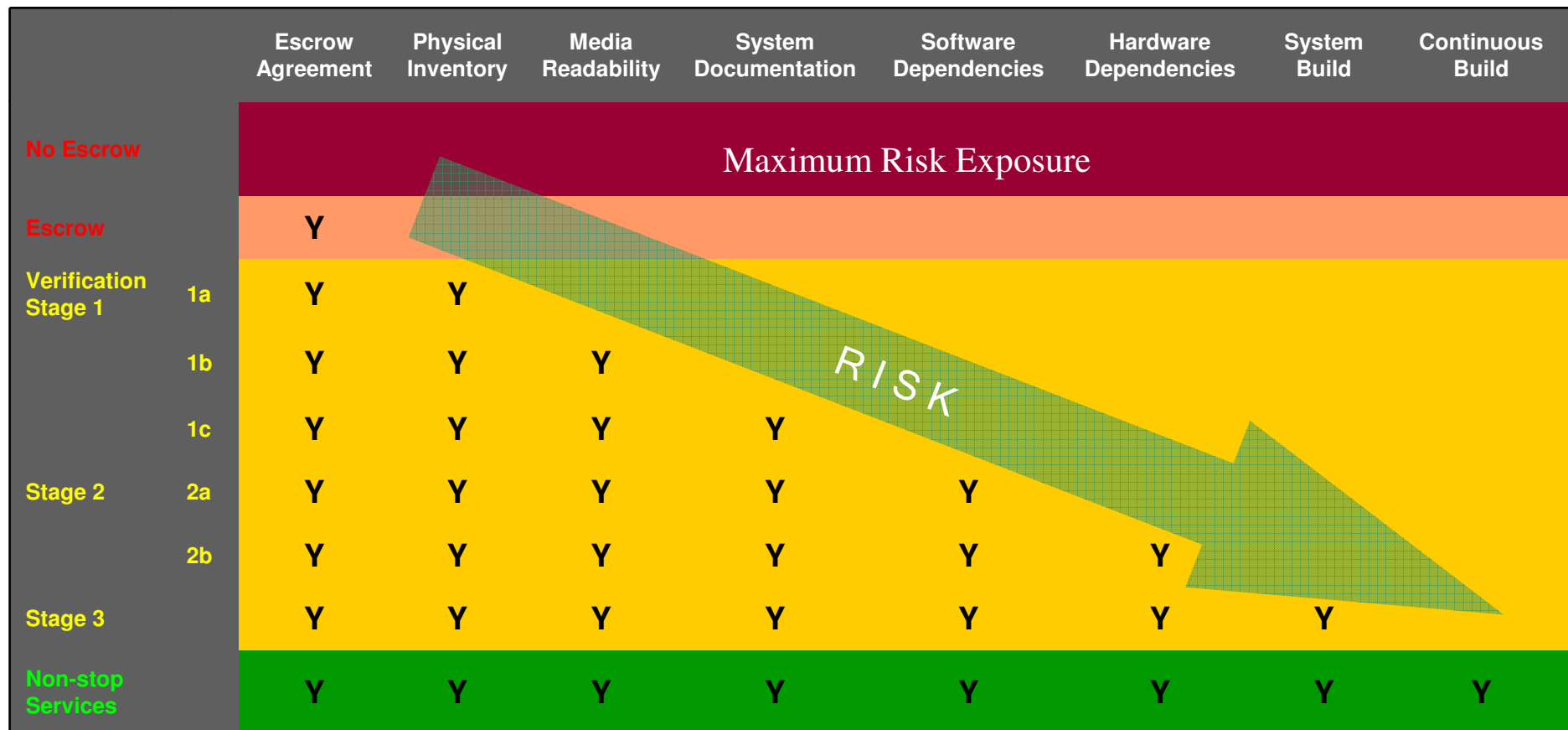
- **Stage 1 Basic**
 - Physical Assessment
 - Media Assessment
 - Documentation and Supporting Information
- **Stage 2 Dependencies**
 - Software
 - Hardware
- **Stage 3 Build and Test (compilation)**
 - File Checksums
 - Code Compilation
 - System Build and Test

Non-stop services

- **Continuous Audit**
 - Follows Stage 3 Validation
 - Ongoing tracking of dependencies
 - Automated alerts
- **Continuous Build**
 - Complete synchronised system build
 - Mirror of customer system
 - Hard disk physically stored in escrow vault
 - Highest availability on triggering event
 - Usually 48 - 72 hours

Risk Mitigation and Services

Risk Area



SUMMARY

- All business critical third party software should be escrowed
- If it is worth escrowing – then verify
- Build processes into global business risk management – not business unit level
- Source code verification is an integral and crucial part of business continuity planning – often overlooked

