nccgroup | SOFTWARE RESILIENCE

Mitigating Third-Party Software Supplier Risk

Tom Sutton, MBA

Why I am Speaking

Thomas Sutton

Global Account Director

- Advise Globally Systemic Financial Services organizations
- Consult on best practices, policy adoption and controls
- Professional Toddler Wrangler

Welcome

What we are covering today:

- Where is the risk?
- Third-Party Software in your Operations
- Software Escrow as a Stressed Exit Plan
- Who should be involved?
- Regulatory Environment
- Recap

Where is the Risk?

nccgroup | SOFTWARE RESILIENCE

Third-Party Software in your Operations

Software Touches Every Part of Business

How many Ops rely on Third-Party Software?

Revenue Supported

Customer Usage

Think about…

- **Revenue Lost**
- **Customer Perception**
- **Regulatory Fines**
- **Organizational Impact**

Where’s the Risk?

- Reliance on Third-Party Software Vendors is at an All-Time High
- Lack of Control (Especially Cloud)
- Lack of Insight

What if the Vendor ends support for your application?

Software Escrow as a Stressed Exit Plan

nccgroup | SOFTWARE RESILIENCE

Software Escrow as a Stressed Exit Plan

01

Software supplier legally agrees to put a copy of the application in escrow

02

Vendor uploads code, access credentials, or replicated instance of your application

03

In the event of bankruptcy, change of IPR failure to maintain, the respective materials are released, and you continue business as usual

Protecting What's Critical

Cloud Adoption, Bespoke solutions, Digitizing Operations

Regulatory compliance

Meet strict third-party on-premise and cloud software compliance laws.

Supply chain resilience

Prepare for the possibility of supply chain failure as well as the opportunity to avoid the ripple effect of disruption.

Migrating to the cloud

Reduce risk for apps where the environment, source code, and data is controlled and managed by the software vendor.

Legal protection

From customer escrow agreements to safeguarding software vendors' property, lawyers must ensure their clients' interests are represented.

Going Deeper

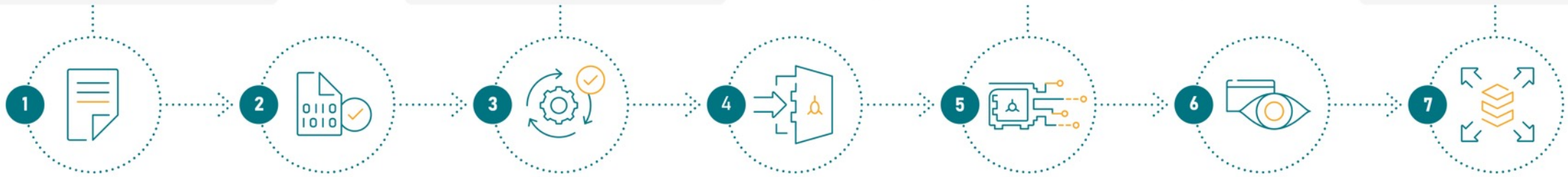
7 Stages of Preparing for Software Vendor Failure

SET-UP
We'll work with both parties to determine how often the materials should be updated, what level of validation should be conducted on the deposit and when the escrow materials should be released.

TEST
We test the source code to assess and identify any security vulnerabilities which exist in the application source code so they can be remediated before they are compiled into the live application and deposited into escrow.

SECURE STORAGE
The deposited materials are placed into a highly secure vault. Our global network of physical and virtual vaults deliver the highest standard of security for the safe deposit and access of business-critical materials in escrow.

RELEASE
If a release condition occurs, we will promptly release the materials to the end-user following the terms agreed in the escrow agreement.



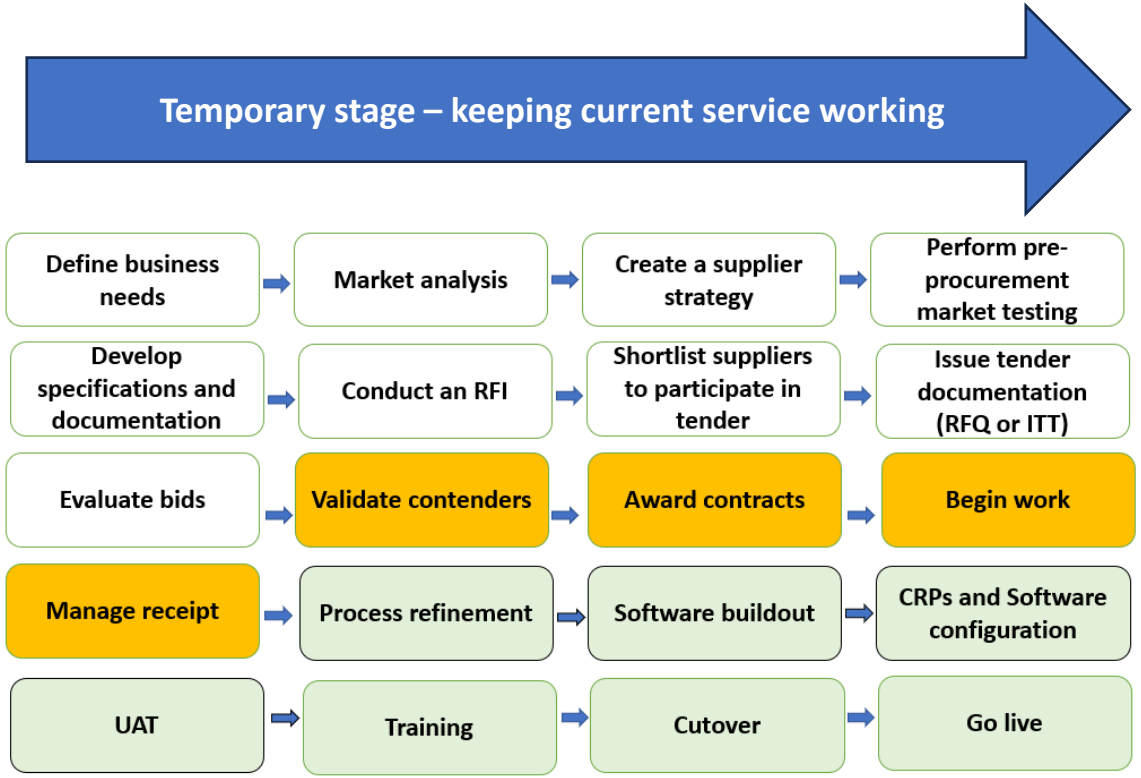
VALIDATE
We'll validate the accuracy and usability of materials held under the escrow agreement so the end-user can redeploy the application themselves, without the need for any additional support from the software vendor.

DEPOSIT
The materials are securely deposited and fully automated through our View platform. View can be synced to all major source code repositories, including Github, Bitbucket, and Gitlab.

GitHub Bitbucket GitLab

MANAGE
Receive live data on the status of deposits and have immediate access to vital documentation in real-time on one platform through View.

Demonstrably successful stressed exit plans



Establish legal right to access and use business critical information

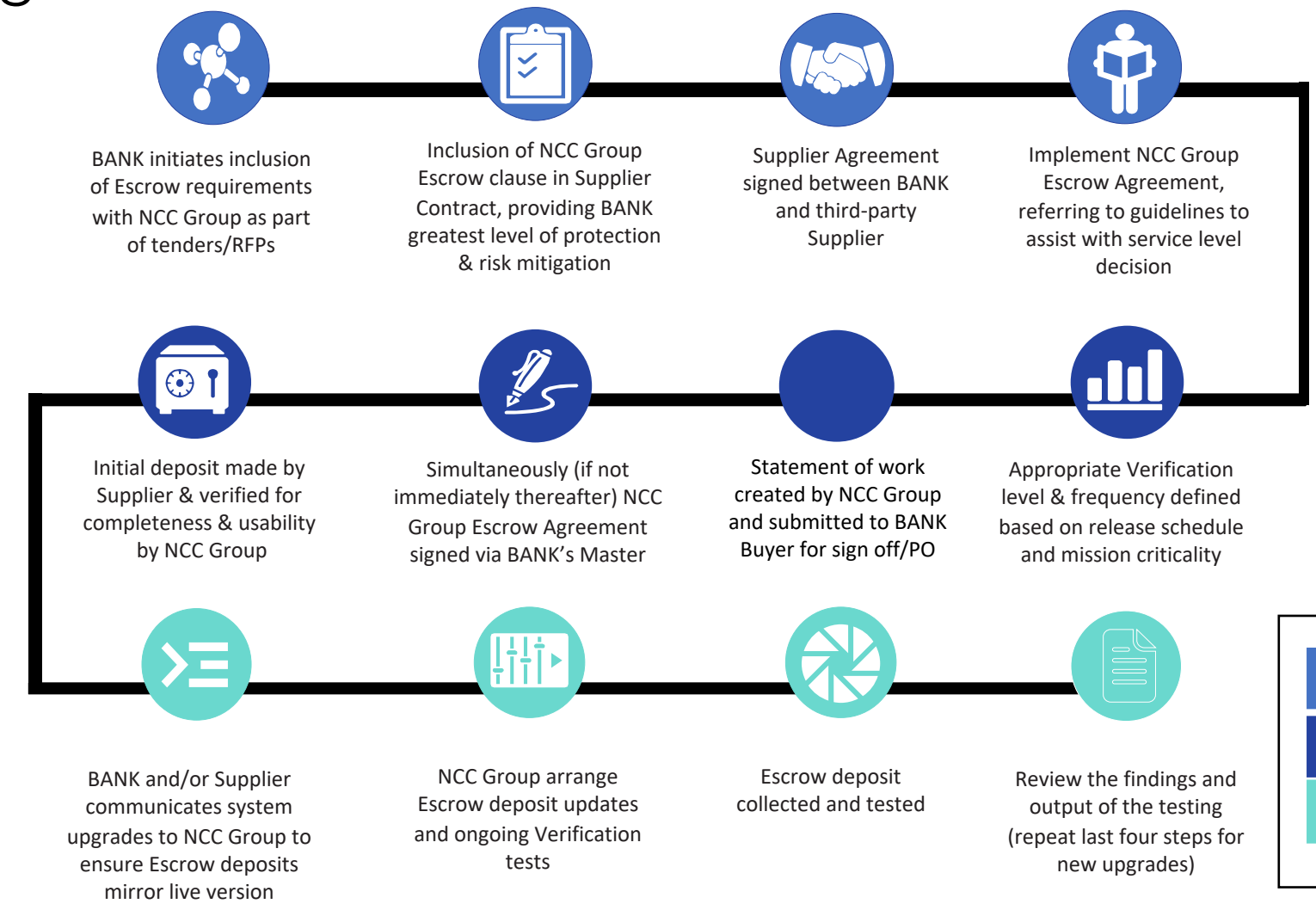
Knowledge transfer

Scenario testing

Who Should be Involved?

nccgroup | SOFTWARE RESILIENCE

High Level Workflow



Meeting regulations

nccgroup | SOFTWARE RESILIENCE

Meeting regulations – PRA SS2/21 (UK)

BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Requirements:

The PRA's Supervisory Statement (SS2/21) consolidates requirements to facilitate greater resilience and adoption of the cloud.

Under the PRA guidelines, firms must have robust continuity measures in place for "important business services" and specifically stipulate that any material cloud outsourcing arrangement must adopt the highest of resiliency options.

Firms should also actively consider temporary measures that can help ensure the ongoing provision of important business services following a disruption and/or a stressed exit, even if these are not suitable long term solutions, (eg contractual or escrow arrangements), allowing for continued use of a service or technology for a transitional period following termination.

How we help:

Our range of Software Escrow Agreements & Verification Services for on-premise and cloud hosted applications provide financial services firms with the legal and technical assurance to bring an outsourced service back-in house or the necessary materials to migrate to another service provider to rebuild the outsourced service

Meeting regulations – DORA (EU)

Requirements:

The EU's Digital Operational Resilience Act means financial institutions in the EU must ensure key requirements to financial entities' contracts which govern their relationship with third-party providers, include provisions on:

- Accessibility
- Availability
- Integrity
- Security
- Guarantees for access, recovery and return in case of third-party failures
- Verification of 'exit strategies'

How we help:

Software Escrow agreements ensure accessibility, availability and recovery in case of third-party failures. And Software Escrow Verification validates a firms' exit strategy to ensure the business continuity plan in place is effective and can be enacted should a third-party provider fail.

Meeting regulations – BaFin (EU)

Requirements:

BaFin has issued regulation guidelines, such as MaRisk (Risk Management), and highlights the below requirements:

- In cases of unintended or unexpected termination of material outsourced activities, firms should adopt possible courses of action to ensure the continuity and quality of outsourced activities
- Regular contingency tests should be carried out in order to verify the effectiveness and suitability of the contingency plan. The business continuity and recovery plans should ensure that normal operations can be resumed within an appropriate timeframe

How we help:

Software Escrow Agreements form a vital part of any business continuity plan as they provide regulated firms with the legal right to access third-party software applications in cases of unintended or unexpected termination of material outsourced services, for example downtime, supplier failure or supplier insolvency.

Software Escrow Verification is implemented to validate the accuracy and usability of the materials held under the agreement and gives a firm the knowledge required to execute their exit plan accordingly ensuring that normal operations can be resumed within appropriate timeframe.

Meeting regulations – FDIC (US)

Requirements:

The Federal Deposit Insurance Corporation (FDIC) is an independent agency created to maintain stability and public confidence in the nation's financial system by addressing risk.

- Business resumption and contingency plans should be in place for all outsourcing agreements.
- Any third-party contracts should have appropriate measures for backing up information and maintaining disaster recovery and contingency plans.

How we help:

Software Escrow Agreements ensure a bank's continuous access to software source code and programs under certain conditions (e.g. insolvency of the third-party).

Software Escrow Verification enables a bank to transition to alternative vendors or bring services in-house to mitigate risk in the event of contract defaults or termination.

Meeting regulations – MAS (Singapore)

Monetary Authority of Singapore

Requirements:

Financial institutions must:

- Ensure providers have risk mitigation and business continuity measures in place.
- Follow strict standards around secure coding, source code review and application security testing.
- Appoint a CIO and a CISO to the board, and train all other board members on technological risk.

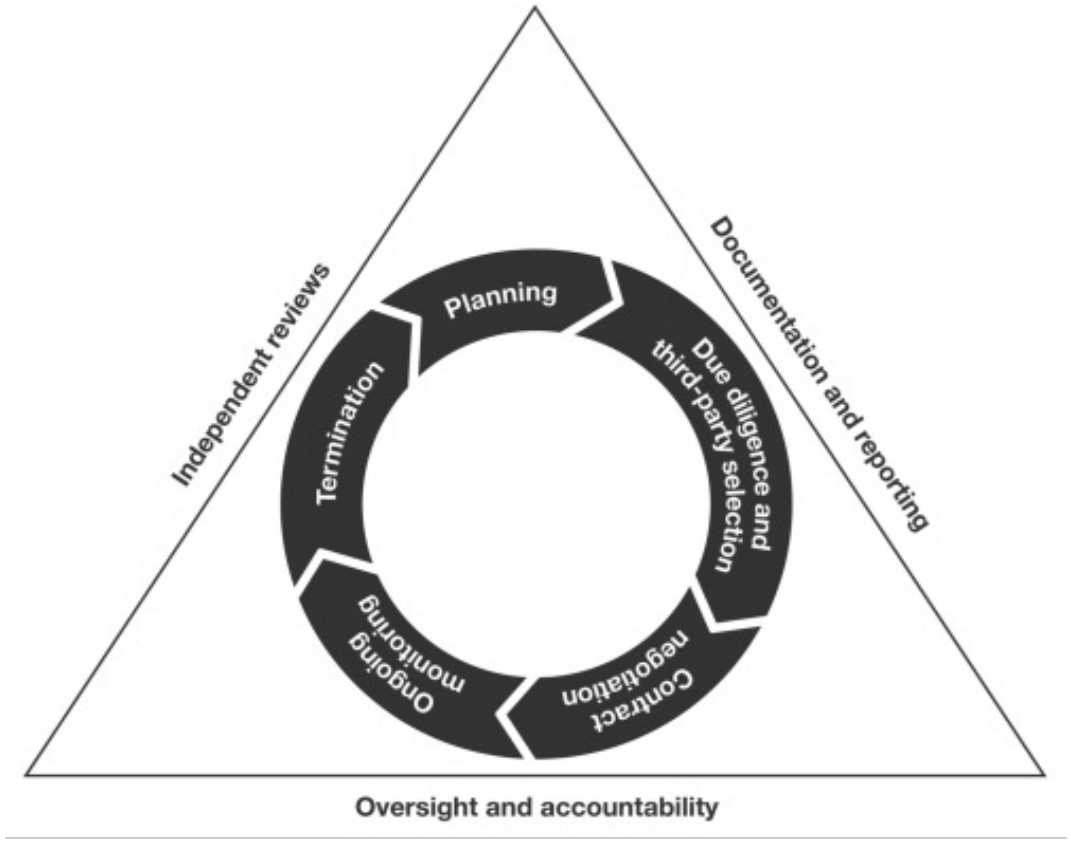
How we help:

We build Software Escrow agreements and Verification Testing into contracts, ensuring that third parties meet a high standard of compliance and due diligence.

Regulatory Patterns

1. Naming of supplier failure, service deterioration and concentration risk
2. Assign owner of the risks
3. Mapping
4. Risk appetite and risk tolerances
5. Build plans
6. Test plans
7. Learn the lessons
8. Proportionality

Stressed exit plans that enable the regulated entity to bring the management of a failed service in house, or, pass the management to a 3rd party



Welcome

What we are covering today:

- Who we are
- Our platform and solutions
- Solving your challenges
- Marketing the Risk – Taking a Group approach
- Stakeholder involvement
- Recap