blueprism®

Robotic Process Automation Software

Compliance and non-repudiation

For financial services organizations

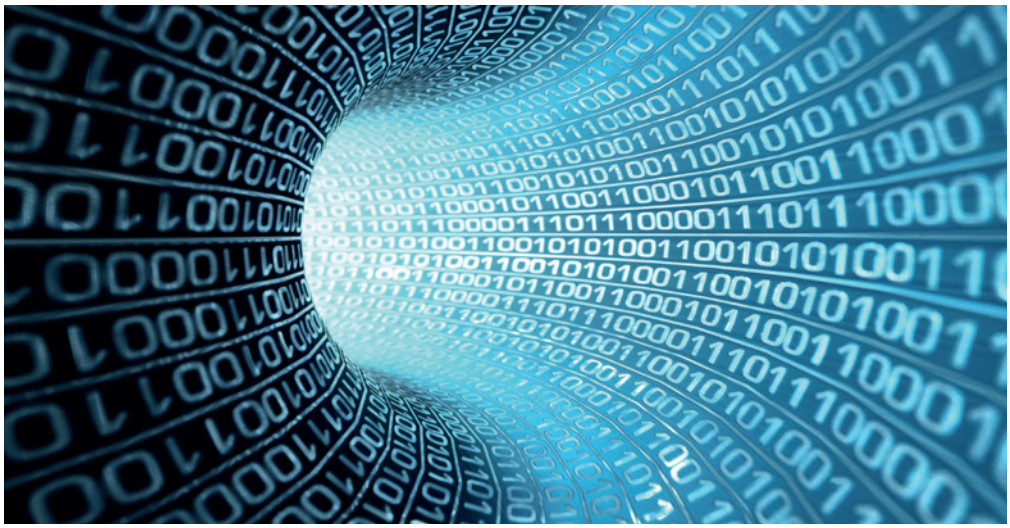
Delivering the **world's most successful digital workforce.**

Context

Financial services organizations operate under strict international and domestic regulation which, in the case of severe breaches, carries potential fiscal and criminal penalties for the institution as well as accountable persons.

blueprism®

What this means for Robotic Process Automation (RPA)



A Digital Workforce requires security, oversight and governance just as a human workforce does.

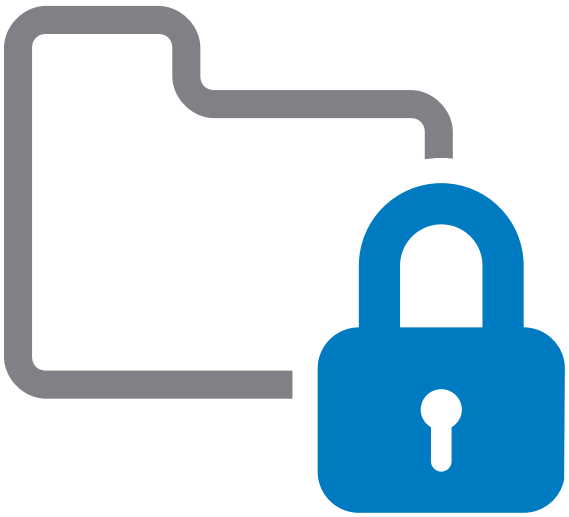
While the vast majority of human employees act with honesty and integrity, the actions of just one unscrupulous employee can have a disproportionate effect on the organization. This is especially the case when he or she has a configurable and flexible Digital Workforce at their disposal.

Possible risks include scaled theft/fraud, cyber attacks such as denial of service, malicious corruption of data and more. **It is imperative therefore, that strict controls are in place as to how robots are configured and how changes are managed and approved.**

Control, Security and Oversight

The detailed software security features that enable a secure environment and methodology for positive change are numerous but will typically be based on the following high level themes:

- **Centrally managed user access control, limiting access to named individuals only**
- **Role based access according to the principle of least privilege**
- **Multi-actor security, such that no individual can make changes without secondary approval**
- **A complete retrospective audit/changelog of all activity, such that accountability and responsibility is made fully visible**
- **Segregation of environments with separate controls governing each**
- **Infrastructural security – a controlled runtime environment that is free from interference, casual inspection or tampering**



Deterrent against misuse

A critical element in the above is the audit trail. This should not be underestimated as behavioural psychology identifies three key issues in driving unscrupulous behavior:

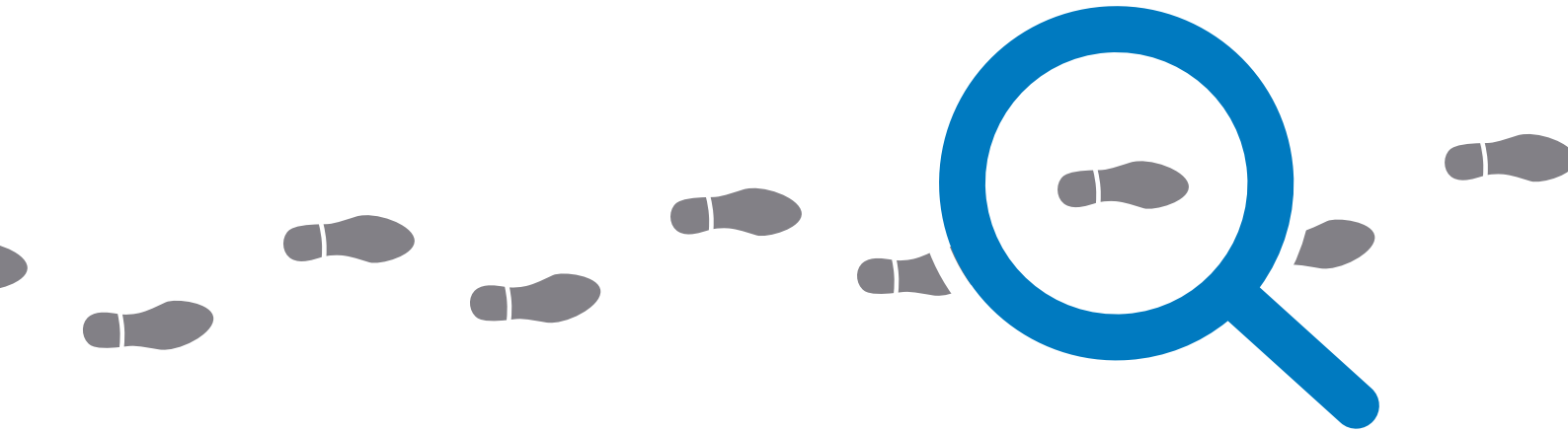
1) the perceived difficulty in executing the crime in question;

2) the size of the incentive (eg the proceeds of crime);

3) the likelihood of being caught (and moreover the likelihood of being held to account once caught)

While a multi-layered security approach can address the first two issues - by increasing the difficulty level required in the wrong-doing and by limiting the available control once a single breach is made - security alone does nothing to address the third issue regarding the likelihood of being held to account. This is where the audit trail provides immeasurable value, by providing a mechanism through which perpetrators can be held to account or errors can be corrected.

Ultimately, the quality and integrity of this audit trail will determine the size of the disincentive: it is those users with the strongest familiarity and working knowledge of the RPA system in question who are most likely to abuse it, so it is very important that they do not feel they have a feasible means of overcoming or defeating that audit trail.



Audit trail attributes

Integrity

An audit trail should be **system generated.** If an audit trail is not system generated then it needs to be user-generated. Any user-generated audit trail is subject to the following critical flaws:

- The user can choose to omit details or indeed "forget" to create one
- The user can deliberately deceive by creating a false audit trail

Centralized management and security

The audit trail should be held centrally and securely to prevent both loss and corruption. In particular because a user-generated audit trail is typically very informal in nature – that is, lacking appropriate levels of Enterprise management, foresight and design - it is likely to have little formality to the way in which that audit trail is held or secured.

It is likely to be vulnerable to two issues:

- post-hoc tampering (eg corruption / deletion) in order to mask wrong-doing
- accidental loss (eg local desktop storage or reliance on a server lacking a backup policy)

Immutability

It should not be possible to delete or tamper with the audit trail in any way, even by a system administrator.

If this is possible then, rightly or wrongly, the system administrator (and anyone else with access to the audit trail) automatically becomes an immediate suspect in each and every event of any irregularities or discrepancies being identified in the audit trail.

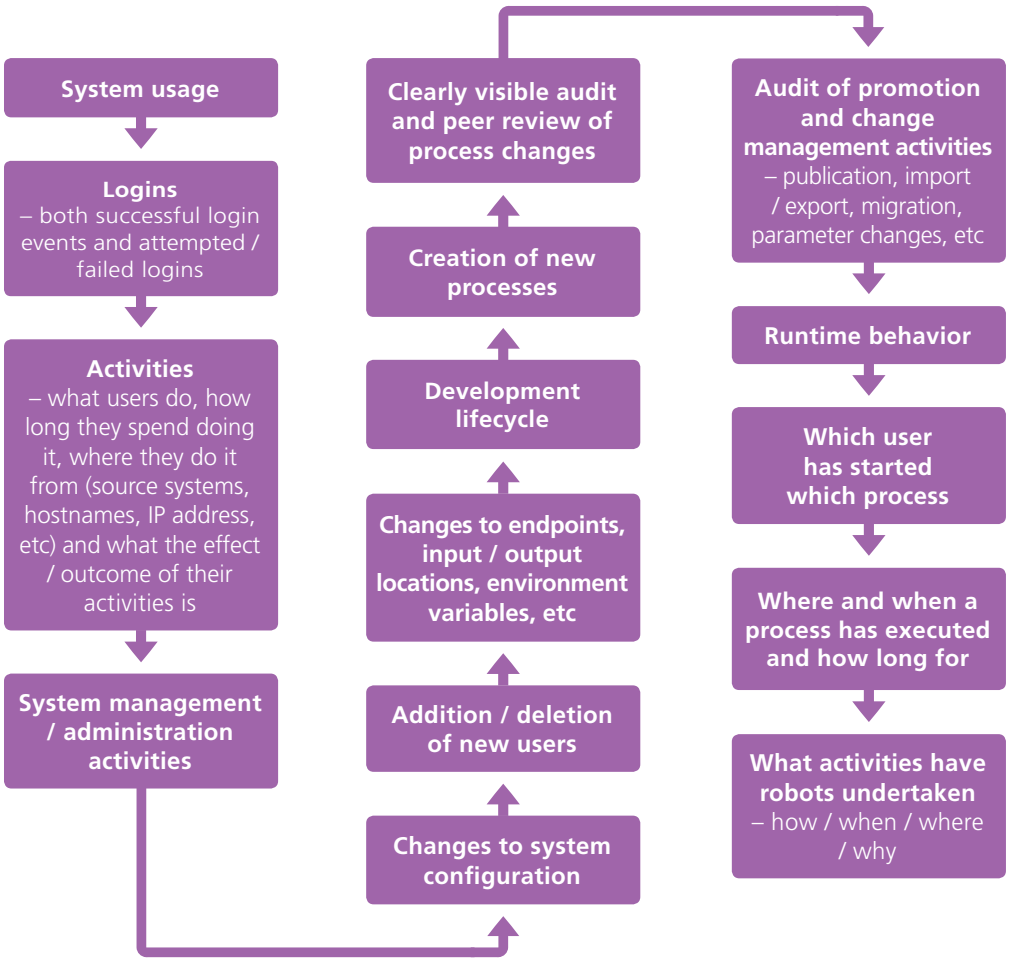
Completeness

An audit trail carries very little value if it contains gaps: any gaps open up uncertainty as to what has taken place in the interim period and undermines potential legal cases.

What to look for in an RPA solution

Minimum scope

The audit trail essentially needs to cover every single piece of human behaviour in the system at any stage. At minimum, an RPA solution should cover:



Without this **full level of oversight**, it would be possible, for example, to develop / create a rogue process in an external environment and then import/run that process and subsequently delete it – all without accountability as to who has done it, how that person obtained user access and what has happened to that process since.

Conclusion

Non-repudiation

The sum effect of the above criteria is **non-repudiation**, something which should be considered an essential and minimal characteristic of any Enterprise RPA platform.

What this means

To repudiate is to deny or argue against something. If an audit trail does not exhibit the above characteristics as a minimum (integrity, security, irrevocability and completeness) then it becomes repudiable: people can challenge its accuracy, claim that it is misleading or incomplete or indeed simply deny any involvement.

At this point, the audit trail lacks the strength and integrity to convict a wrong-doer or fix a serious error.

In turn, the compliance officers within a financial services organisation face the uncomfortable and unfortunate position of having to explain how and why a software platform was chosen that allowed such a sequence of events to take place.