

MERLYNN

TOM Digital Twin AI - Augmenting expert resources  
for more efficient Information Security Risk Reviews

July | 2022

# Quarterly Bulletin

Information/Data Security Risk Management

The threat of a Cyber Attack or Data Breach ranked as the number one risk facing financial institutions in 2022 and within the top 10 risks facing all industry sectors.

(source Aon's 2021 Global Risk Management Survey)

Valuable data that hackers are seeking to exploit includes not only much publicized personally identifiable information but also organizational intellectual property and legally privileged information.

## Information Security Risk Reviews

One of the data security risk management policies organizations have adopted is a security due diligence assessment or information security risk review. Information security (infosec) teams perform security due diligence reviews on all new and existing vendors, technologies, applications and systems to identify and mitigate any potential vulnerabilities.

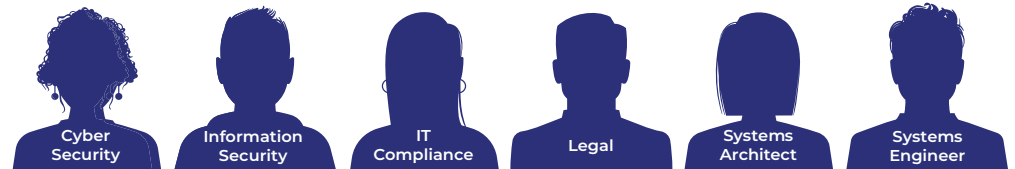
Complexity and reliance on highly skilled subject matter experts to appropriately analyze risk makes current assessment processes extremely time consuming, and inefficient. Depending on availability of skilled resources and backlogs, reviews can take days, weeks or even months to be completed.

While risk reviews are necessary to comply with legislation and manage risk, organizations face a challenge in balancing risk management with efficiency and service delivery.

## TOM Digital Twin Solution

By replicating the knowledge of cyber security, information security, systems architects and IT compliance experts, decision-making Digital Twins enable organizations to scale scarce resources to more efficiently process risk assessments without compromising risk.

Panel of Digital Twins - access to real-time expertise



Digital Twins, created with Merlynn's Tacit Object Modeler (TOM) technology, think and respond to a problem as their human counterpart would - only exponentially faster. The Twin ingests the information needed to make the decision, processes this in milliseconds, and responds as the human would.



Real-time access to the expertise needed to appropriately review and manage the risk enables organizations to automate information security risk reviews, enhancing efficiencies and reducing risk.

# The Challenge

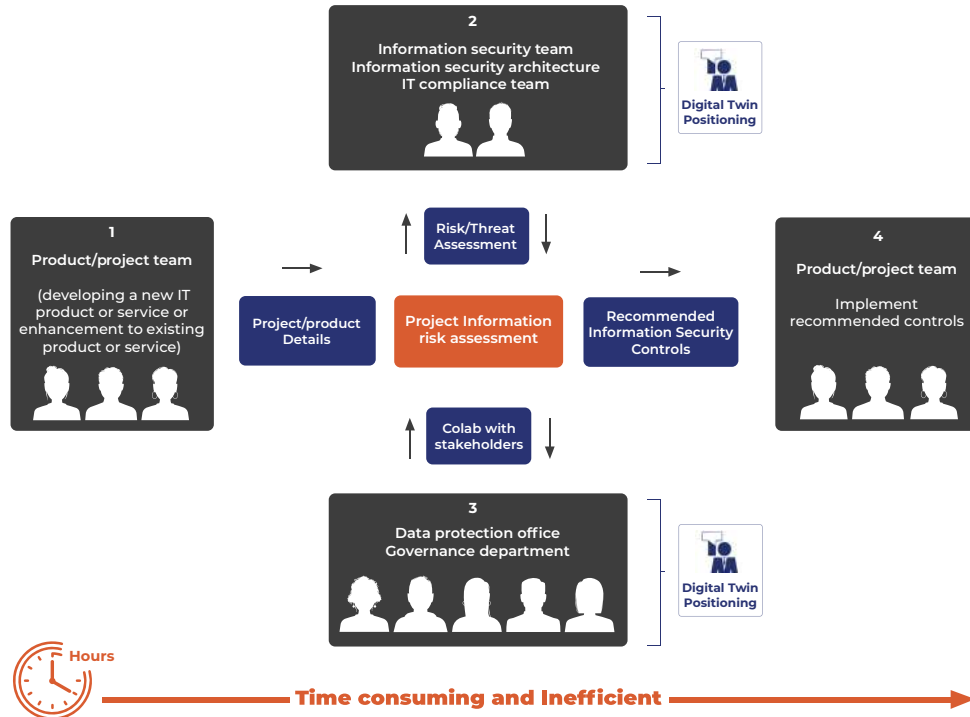
## Existing Assessment Process

A review comprises a detailed assessment for cyber attack threat and information security risk. Reviews cover multiple risk factors including:

- ✓ Data
- ✓ Integration
- ✓ Availability and integrity
- ✓ Infrastructure
- ✓ Privacy & access restrictions
- ✓ Applications
- ✓ Cloud
- ✓ Special systems
- ✓ Governance
- ✓ User Authentication

To appropriately analyze risk, subject matter experts from each of these areas must provide input. In order to develop sustainable and resilient IT products, recommendations need to support organizational policies and standards, as well as data governance regulations.

The diagram below is a high-level representation of the tasks/experts involved in a typical information security risk assessment



1. Project teams submit IT projects (new or change requests) to the infosec team.
- 2 & 3. Various subject matter experts including security, architects, compliance and governance experts assess risk and provide recommendations.
- 4: Outcomes and required changes and controls are fed back to the project team to be implemented prior to going live. Infosec teams monitor and test that recommendations have been implemented.

On-going security reviews are required for higher risk applications and technologies.

## Reviews are:

- Resource heavy** - requiring domain knowledge of various subject matter experts to identify and remediate any potential security vulnerabilities.
- Time consuming** - depending on volumes and backlogs, delays vary from hours to months.
- Costly** - needing to be performed by highly skilled resources.
- Potentially inconsistent** - cyber security assessments differ based on the analyst completing the assessment.
- Repetitive** - continuous assessment of new systems and changes to existing systems are required.

Inefficiencies and delays lead to frustration for business units wanting to adopt new technologies or enhance existing systems.

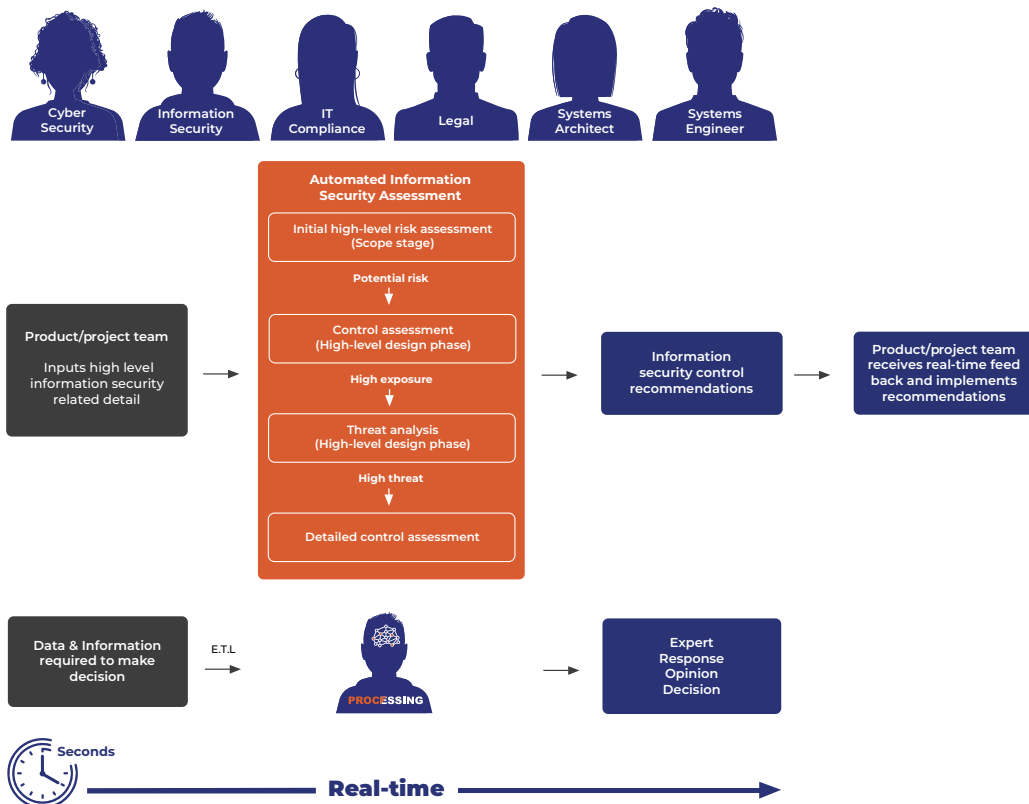
## A Smarter Approach

### Digitally replicating the skills required to perform assessments

Organizations are deploying panels of decision-making Digital Twins (cyber security analysts, information security officers, system architecture and IT compliance resources) to perform assessments and monitor potential data risk in real-time.

The Diagram demonstrates how a panel of Twins enables organizations to more efficiently process/automate security risk assessments.

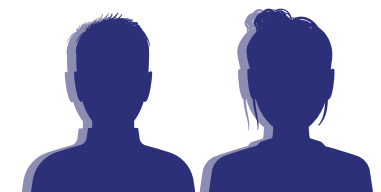
Panel of Digital Twins - access to real-time expertise



1. Digital Twins of the necessary resources are deployed within the process to assess information security risk.
2. The product teams submit information required for the assessment, this is parsed through the panel of Digital Twins for real-time response.
3. Recommended controls are generated instantly.
4. These can then be implemented in existing systems by the project team within hours or added to the project plan for new systems.

### Automating the risk assessment process:

- Delivers faster more consistent and accurate assessments/reviews, reducing risk, and enhancing efficiency.
- Enables organizations to meet compliance and reporting obligations through transparent audit trails for decision making.



Creating a Digital Twin