MERLYNN

2022

Digital Twins
in Information Security Risk Reviews

Augment your expert resources for more efficient Information Security Risk Reviews

Information Security Risk Reviews

Information security risk reviews ensure that data, including personally identifiable information, organizational intellectual property and legally privileged information is protected. Information security (infosec) teams perform data security assessments on all new and existing vendors, technologies, applications and systems to identify and mitigate any potential vulnerabilities.

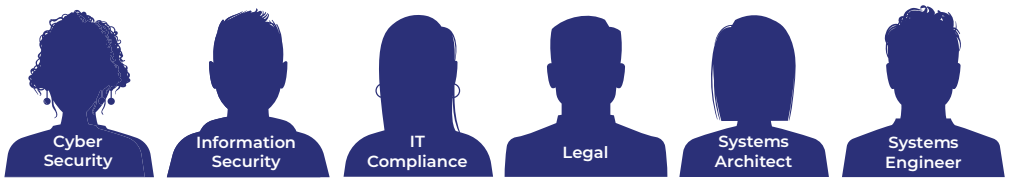
Complexity and reliance on highly skilled subject matter experts to appropriately analyze risk makes current assessment processes extremely time consuming, and inefficient.

Depending on availability of skilled resources and backlogs, reviews can take days, weeks or even months to be completed.

TOM Digital Twin Solution

By replicating the knowledge of information security experts, systems architects and IT compliance experts, decision-making Digital Twins enable organizations to scale these valuable 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 it 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 reviews.

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. On-going security reviews are required for higher risk applications and technologies. Inefficiencies and delays lead to frustration for business units wanting to adopt new technologies or enhance existing systems.

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.

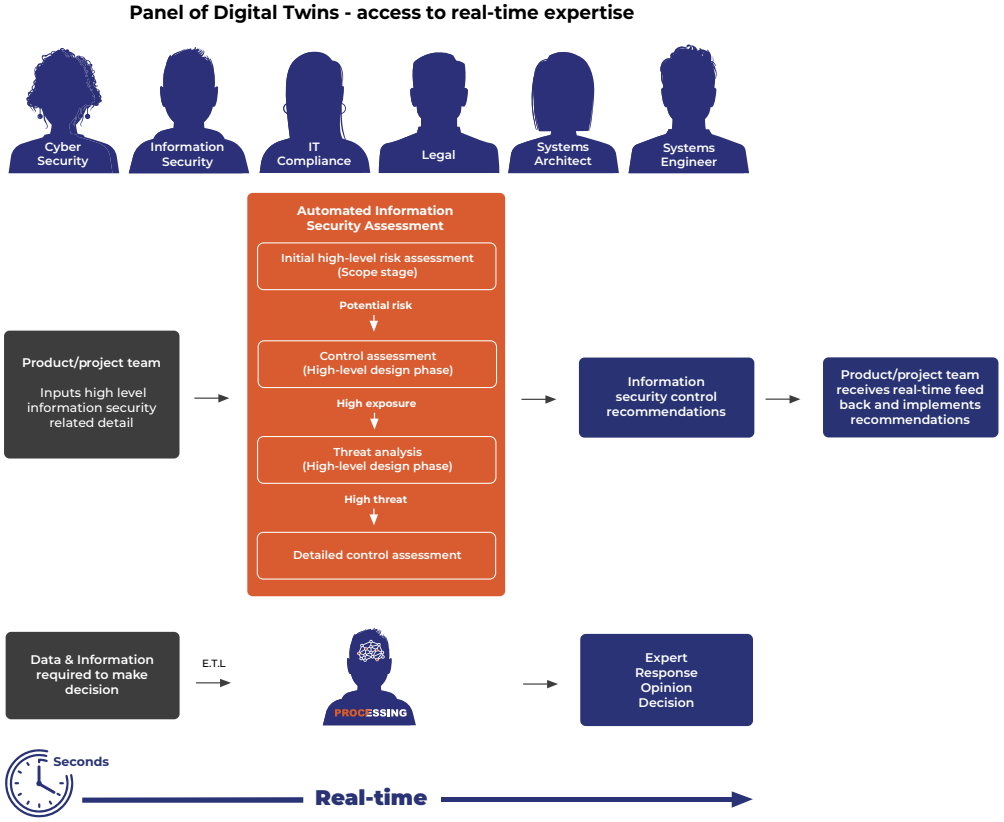
Contact us for more information : **info@merlynn-ai.com** | www.merlynn-ai.com

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 on the right demonstrates how a panel of Twins enables organizations to more efficiently process/automate security risk assessments.



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:

- Faster, more efficient reviews enabling ongoing analysis and improving time to production for new innovations.
- More consistent and accurate assessments, reducing risk.
- Resource efficiencies - more productive use of expert time.
- Transparency - decision audit trail for compliance & reporting.

Contact us for more information : **info@merlynn-ai.com** | www.merlynn-ai.com