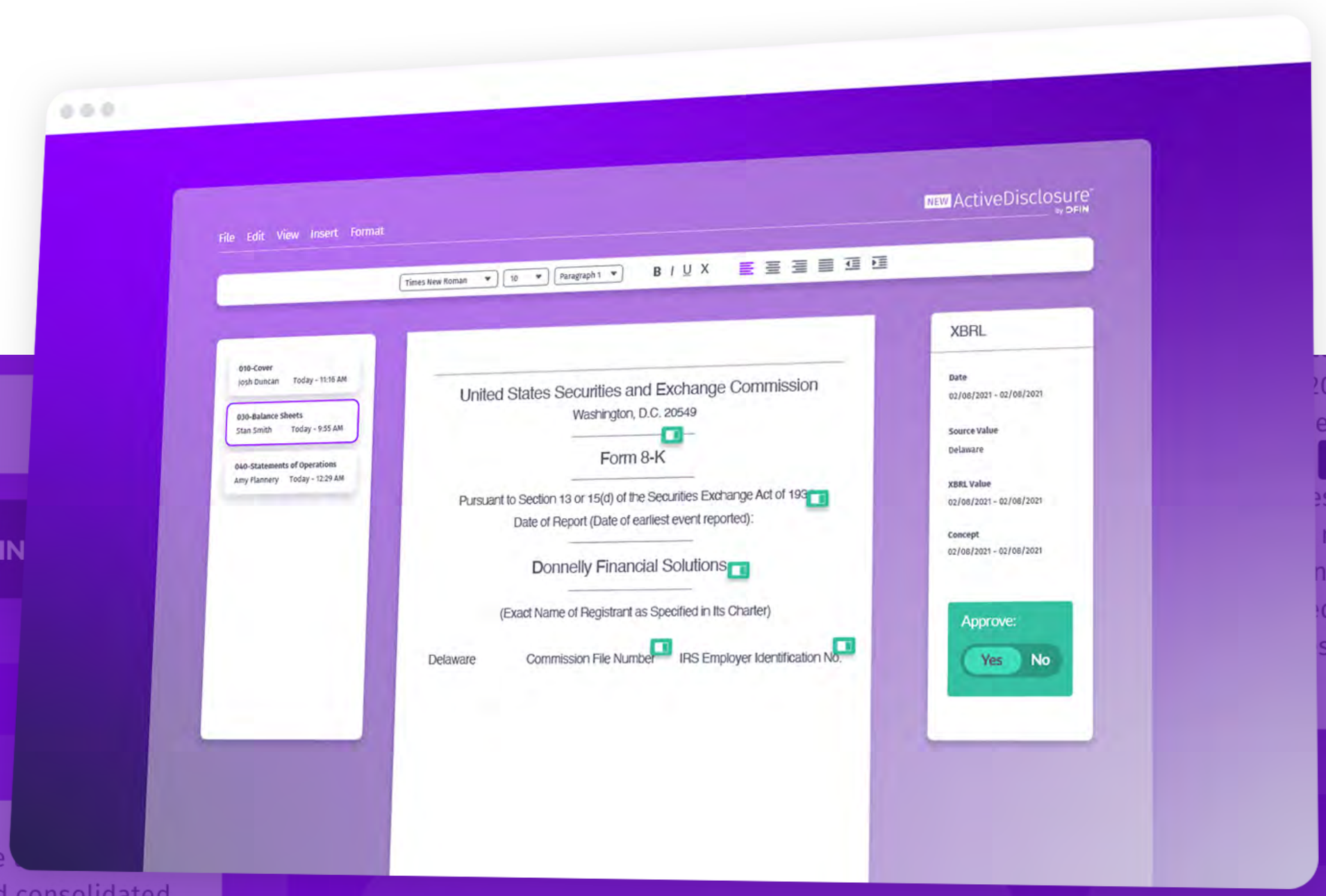
NEW ActiveDisclosure℠ by DFIN

Product Security Overview

NEW ActiveDisclosure℠ by DFIN

The **new ActiveDisclosure (new AD)** is purpose-built for secure financial reporting and SEC filing. Built by and for experts, the new AD SEC reporting software is designed to be faster, smarter, and more secure than ever before. It gives teams a robust set of streamlined features for safe real-time collaboration and accurate financial reporting.

Donnelley Financial Solutions (DFIN) is a leader in risk and compliance solutions, providing insightful technology, industry expertise and data insights to clients across the globe.



DFIN'S CYBERSECURITY OVERVIEW

The **DFIN Information Security Program** is designed to ensure data protection, supply chain security, and enterprise cybersecurity throughout the environment. The program is based on business requirements derived from:

Assessing

security risks to the organization.

Defining

the legal, statutory, regulatory, and contractual requirements that DFIN and its business partners, contractors, and service providers must satisfy.

Delineating

the principles and objectives for operational information processing.

Information Security for the new AD is achieved by implementing a set of controls, which consist of policies, processes, procedures, organizational structures, and software functions.

Controls have been established to minimize risk and protect information assets required to meet the operational, financial, and regulatory requirements to safeguard client data and privacy. Information security is characterized as the preservation of:

SECURITY

to protect assets from external and internal threats

AVAILABILITY

to prevent disruption of service and productivity

CONFIDENTIALITY

to prevent unauthorized disclosure of sensitive information

CONTROLS APPLIED TO OUR PRODUCTS

Organizational Controls

DFIN's robust organizational controls ensure that security is addressed as a part of all software development at DFIN by integrating security practices and generating security and complacence artifacts throughout the process. The **advantages** in doing so are:

- Reduction in vulnerabilities, malicious code, and other security issues.
- Mitigation of potential impacts of vulnerability exploitation throughout the product's lifecycle.
- Evaluation of root causes for vulnerabilities to avoid future occurrences.

NEW ActiveDisclosure℠ by DFIN

Leveraging S-SDLC (Secure Software Development Life Cycle) and applied security risk frameworks such as NIST CSF, as well as adherence to AICPA Trust Service Principles, guide DFIN's development efforts and ensure application security within the new AD.

From an accountability perspective, security awareness, data privacy, ethics, and code of conduct are instilled into DFIN team members.

NEW ActiveDisclosure℠ by DFIN

Security by Design

The new AD is a Software as a Service (SaaS) offering deployed in Microsoft Azure. DFIN applies the principle of "security by design" and has applied multiple cloud security standards including but not limited to:

Strong perimeter security controls to reduce the attack surface and prevent unauthorized access.

Static and dynamic application security testing (SAST/DAST) to embed security early into the S-SDLC.

Encryption at rest and in transit using TLS1.2 and strong encryption algorithms like AES-256.

Annual penetration tests by an authorized independent third party.

Single Sign-On (SSO), Multifactor Authentication (MFA), and robust role-based access control (RBAC) ensure the least privileged access to assets and resources in the Azure environments.

Centralized log collection and continuous security monitoring to identify, correlate, detect, and respond to security events.

DFIN further applies Azure best practices for network security, identity management, access control, database security, data security and encryption, and operational security.

For more information on Microsoft Azure Security, please visit **https://docs.microsoft.com/en-us/azure/security/.**

Commitment to Security

The new AD ensures the integrity of client data and access through industry standards and best-in-class security provisioning. The chart below highlights security considerations for original and new ActiveDisclosure.

Security	New AD	Description
Document ecryption at rest	YES	Uses AES-256bit encryption for data at rest
Information encryption in transit	YES	Uses TLS 1.2
Database file encryption	YES	The new AD uses AES-256bit (original AD uses TDE)
Access encryption	YES	HTTPS (Hypertext Transfer Protocol Secure)
Key vault storage	YES	Azure Key Vault for storing keys used for application operation
Identity Access Management – Multi-Factor Authentication	YES	Supported
Identity Access Management – Single Sign-On (SSO)	YES	Supported
Penetration Testing	YES	Methodic and exhaustive annual test with priority remediation of any security vulnerability issues
Static Application Security Testing (SAST)	YES	Performed continuously on software with priority remediation of any security vulnerability issues
Dynamic Application Security Testing (DAST)	YES	Performed regular on infrastructure with priority remediation of any security vulnerability issues
Threat Management	YES	Performed continuously on infrastructure using tools such as CarbonBlack and Symantec Endpoint Protection (SEP)

DevOps, Cloud Development and Architecture

Development on the new AD embraces modern S-SDLC and Continuous Integration / Continuous Deployment (CI/CD) best practices aligned to a multi-environment (Integration, Quality Assurance, Staging, and Production) release promotion process.

These practices include architectural definition and review of new functionality embracing "design for failure", API driven design, mandatory code reviews, automated testing of new and changed functionality, regression testing of new and changed functionality, and performance testing.

Modern log analysis and application and database performance monitoring tools are leveraged as part of the development process to prevent escape defects. If adverse client-impacting issues do escape to production, a rigorous Root Cause Analysis (RCA) process is followed to identify the root cause and, when needed, prioritize rapid incorporation of design and code changes to prevent a similar reoccurrence.

NEW ActiveDisclosure℠ by DFIN

In Summary

The new AD offers an extensive, yet easy-to-use interface aimed at making financial reporting workflows smoother, faster, efficient, and secure.

DFIN understands the importance of maintaining a comprehensive and robust Information Security Program that spans network, system, application, and data security singularly focused on safeguarding our products and our client's data. DFIN aims to be a trusted partner to our clients.

CONTACT US

thenewAD@dfinsolutions.com
+1 800 823 5304

DFIN