

Archer[®] Regulatory Content Analysis

Use Case for Regulatory & Corporate Compliance Management

The Challenge

In today's complex regulatory environment, governmental and industry bodies frequently make changes to laws, regulations and industry requirements. Organizations face a daunting task in keeping abreast of these changes. Regulatory change-related activities result in millions of hours of research and paperwork each year, with most of that work being done manually in spreadsheets. This work requires that individuals that have knowledge of external regulations and internal controls and requires experience and practice to achieve efficiency and accuracy.

While organizations are compelled to establish processes to identify regulatory changes and implement measures to maintain compliance, the growing volume of regulatory data from a wide variety of sources makes it difficult to identify, prioritize and respond to the issues that impact your organization.

Overview

Archer[®] Regulatory Content Analysis enables compliance analysts to more quickly and efficiently focus on specific areas of regulations that impact the organization. Incorporating patent-pending technology, Archer Regulatory Content Analysis utilizes natural language processing and machine learning to analyze how an organization maps existing regulations to controls. It leverages adaptive learning capabilities of the algorithm to identify and recommend control changes specific to the organization's control structure.

With Archer Regulatory Content Analysis, organizations can more effectively identify regulatory changes and ensure compliance while minimizing resource-intensive manual processes.

Key Features

- Automatic suggestions of applicable controls for new regulations based on controls environment.
- Natural language processing and machine learning to process text-based regulations.
- Highlighted similarities for new and existing regulations for analysts' reference.
- Unmatched content can be manually mapped utilizing advanced search and mapping features.
- SaaS-based offering available for Archer on-premises, hosted, and SaaS implementations.

Key Benefits

With Archer Regulatory Content Analysis, you can:

- Accelerate the process of analyzing new and updated regulations.
- Gain greater efficiency by focusing regulatory change management on what applies to your organization.
- Intelligently automate the resource-intensive process of sorting through regulatory change documentation and determining business impact.
- Ensure consistency of regulations analysis across the organization.

AC-04 (1) INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY ATTRIBUTES

Use [Assignment: organization-defined security attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions. Supplemental Guidance: Information flow enforcement mechanisms compare security attributes associated with information (data content and data structure) and source/destination objects, and respond appropriately when the mechanisms encounter information flows not explicitly allowed by information flow policies. For example, an information object labeled Secret would be allowed to flow to a destination object labeled Secret, but an information object labeled Top Secret would not be allowed to flow to a destination object labeled Secret. Security attributes can also include, for example, source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security attributes can be used, for example, to control the release of certain types of information.

Mapped standards:

ATCS-254 0.38 ATCS-528 0.94 ATCS-261 0.45 ATCS-042 0.75

ATCS-413 0.38

Similar Auth-Sources:

Auth Source Details	Mapped Standard Details	Similar Auth-Source Details
<p>Suggested Tags</p> <p>List of tags assigned to the auth-source</p>	<p>Grouping</p> <p>Information Security Program Management</p>	<p>0.87 [INSTR005394_T01_504_SS001] AC-04 (1) INFORMATION FLOW ENFORCEMENT OBJECT SECURITY ATTRIBUTES</p>
<p>Sub Section Name</p> <p>AC-04 (1) INFORMATION FLOW ENFORCEMENT OBJECT SECURITY ATTRIBUTES</p>	<p>ATCS-254 Security Requirements for Electronic Data Interchange (EDI) Connections</p> <p>All Electronic Data Interchange (EDI) connections should be properly reviewed and authorized by Information Security. EDI connections should meet the following minimum security requirements:</p> <ul style="list-style-type: none"> • EDI arrangements and trading partner agreements should be monitored continually to ensure accuracy • All EDI transactions should be processed using industry standards (e.g., UCS, WINS and X.12) • Enforce information sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared. • Implements information search and retrieval services that enforce organization defined information sharing restrictions. • classifications should not use reifiable media. 	<p>Sub Section Name</p> <p>AC-04 (1) INFORMATION FLOW ENFORCEMENT OBJECT SECURITY ATTRIBUTES</p>
<p>Sub Section Description</p> <p>Use [Assignment: organization-defined security attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions. Supplemental Guidance: Information flow enforcement mechanisms compare security attributes associated with information (data content and data structure) and source/destination objects, and respond appropriately when</p>		<p>Sub Section Description</p> <p>The information system uses [Assignment: organization-defined security attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.</p> <p>Supplemental Guidance: Information flow enforcement mechanisms compare security attributes associated with information (data content and data structure) and source/destination objects, and respond appropriately (e.g., block, quarantine, alert administrator) when the mechanisms encounter information flows not explicitly</p>

Discover More

Archer is a leading provider of integrated risk management (IRM) solutions that enable customers to improve strategic decision-making and operational resilience with a modern technology platform that supports qualitative and quantitative analysis driven by both business and IT impacts. As true pioneers in GRC software, Archer remains solely dedicated to helping customers manage risk and compliance domains, from traditional operational risk to emerging issues such as ESG. With over 20 years in the risk management industry, the Archer customer base represents one of the largest pure risk management communities globally, with more than 1,200 customers including more than 50% of the Fortune 500.