

## How Financial Institutions Can Lower Business Risk While Reducing Audit Fatigue

Improve your cyber risk awareness and better manage the time, costs, and effort of your IT security audit process with **Xacta**® from Telos Corporation.

Financial services organizations are struggling to manage cyber risk and IT security compliance. They are trying to handle this complex, vitally important work with legacy GRC platforms, which weren't built and were never intended to manage the unique challenges of IT risk and compliance.

As a result, these firms are wasting precious time trying to force their GRC tool to support their audit processes while also losing money — in salaries for IT security personnel to deal with audit preparation, and in fines levied at the national, state, and local level.

The burden of managing IT security and privacy compliance without the right tools for the job has grown so exhausting that it's earned its own name: *audit fatigue*.

**85%** of security professionals say the many cumbersome processes for different types of audits are the most time-consuming task on their plates.

*What if they could spend that time managing threats?*

### The Harsh Reality of Audit Fatigue

**\$ \$4 million:** Average amount financial institutions spend each year on IT security compliance and privacy regulations

**\$ \$10 million-\$100+ million:** Amount of OCC and other fines for lack of IT audit controls

**\$ \$15 million:** Average amount firms in all industries spend on the consequences of non-compliance



**14:** Average number of different regulations organizations must comply with



**62:** Working days per quarter responding to audit evidence requests



**78%:** Security personnel who report dread when their organization is audited



**85%:** Security personnel who believe compliance in the cloud is an issue

### The need for a solution is reaching crisis levels – GRC isn't cutting it.

To ease the burdens imposed by today's continuous audit cycles financial services organizations are scaling up their internal cybersecurity and compliance teams. But no amount of extra human resources can keep up with the scope and complexity of compliance under these conditions. The majority of organizations – 84% – report that their IT audit processes are cumbersome and time consuming. And more than three in four security professionals personally dread their organizations being audited.



## Xacta: Purpose-built IT Risk Management for the Financial Services Enterprise.

*Reduce compliance and audit time and effort by up to 90 percent with payback in less than a year.*

**Xacta from Telos Corporation** is an enterprise IT risk management (ITRM) platform that lowers the cost and effort of compliance while continuously monitoring your security posture for today's continuous audit environments.

As the system of record for IT risk management across your organization, Xacta streamlines and automates the key processes in compliance monitoring and reporting for on-premises, cloud-based, and hybrid systems. It automatically aligns multiple frameworks to reduce the redundant effort that audits require for meeting numerous standards, and it aggregates data at scale from the leading security products to report on your entire IT environment.

You may already have a legacy GRC tool, but it isn't adequate for these challenges of IT security compliance. For today's continuous audit cycles, you need the powerful capabilities of Xacta to complement your existing GRC and to accommodate the unique demands of cybersecurity assurance.

### **Xacta: Three capabilities that speed and ease the audit process.**

Xacta empowers you to re-envision and transform the way you do IT audits and compliance, saving time and money and freeing your security and audit personnel to focus on strategic tasks. Here are the three key capabilities that make Xacta the unique solution for ending the burden of audit fatigue.



**1 Automated control testing for today's never-ending audit cycles.** Financial institutions have to monitor and report on thousands of security products that generate millions of data points. This manual effort requires hundreds of dedicated IT security staff to manage the products, generate the test data, and audit the results. Legacy GRC platforms aren't built to support this work.

Xacta reduces this effort and expense by enabling automated controls testing at scale. Xacta aggregates real-time security data from the third-party sensors and sources across your network via open API, normalizes the results into a single view, and maps the results to the relevant controls.

Then, you can automatically enable testing against millions of random data points for control testing in



*How long it takes to generate six million random control test data samples:*

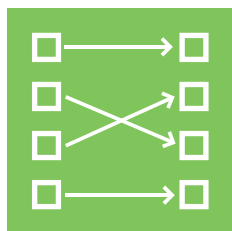
**Before Xacta:** 45 days with manual tasks and spreadsheets

**With Xacta:** 1-5 days with security data aggregated and automatically generated at scale

days, not weeks – slashing up to 95% of the time from request to delivery. Xacta enables near real-time and on-demand control effectiveness attestation and reduces the time needed to analyze and confirm findings across hundreds of thousands of assets. That gives your IT security team more time to focus on mitigating threats and managing risk rather than on repetitive manual audit tasks.



All security scanning results reside in a central repository that serves as a single validated source of audit evidence that can be correlated to your GRC governance framework. Xacta also feeds customizable dashboards that give your test, audit, and management teams the at-a-glance insights they need for analysis and understanding of trending security issues. Xacta's ability to increase ongoing awareness of vulnerabilities and adherence to information security policies and standards helps you meet the continuous monitoring requirements of the leading compliance standards and reduces the burden of today's continuous audit cycles.



## 2. Automatically aligns and maps your overlapping financial standards.

Financial institutions face a large and growing number of overlapping security standards and compliance

frameworks. Xacta's extensive policy library contains the security controls that most often apply to banks, insurance companies, and other financial services firms. Its industry-unique Predictive Mapping™ capability crosswalks one

standard to another for one-to-many mappings that enable you to test once and comply with multiple standards without redundant effort. And, unlike conventional GRC tools, Xacta includes pre-defined workflows around your standards to

### Xacta integrates controls, standards, and frameworks for "test one, comply with many" capabilities:

FSSCC	FMFIA	PCI-DSS
FFIEC	ISO 20022	Privacy Regulations
FFMIA	NIST Controls	SOC 2
FINRA	NYDFS	SOC for Cybersecurity

automate compliance processes common to financial services organizations. They can be easily tailored to your requirements and IT environment instead of forcing you to adjust to their limitations as other offerings do. Xacta workflows provide a collaborative environment where security, audit, compliance, and management personnel can work together rather than separately in the compartments of a stove-piped process.

## Xacta and the Three Lines of Defense

The "Three Lines of Defense" model is the Institute of Internal Auditors' framework for managing operational risk. Its principles also apply to the management of cyber risk, which poses distinct challenges to financial services organizations. Xacta provides the unique capabilities needed to manage and gain visibility into your IT security environment as part of your overall compliance and audit management function.

LINES OF DEFENSE	XACTA BENEFITS
<p><i>First Line of Defense:</i>  <b>Operational Management</b>                      Functions that own and manage risks</p>	<ul style="list-style-type: none"> <li>Real-time operational awareness of IT risk</li> <li>Reports and dashboards oriented to operational requirements</li> <li>Options for mitigating IT risk as needed</li> </ul>
<p><i>Second Line of Defense:</i>  <b>Risk Management and Compliance</b>                      Functions that oversee risks</p>	<ul style="list-style-type: none"> <li>Single source of truth for cyber risk management and compliance</li> <li>Identify and monitor IT risk in real time with security-oriented interfaces and reporting</li> <li>One-to-many mapping for integrated compliance with all relevant regulations and frameworks</li> </ul>
<p><i>Third Line of Defense:</i>  <b>Internal Audit</b>                      Functions that provide independent risk assurance</p>	<ul style="list-style-type: none"> <li>An auditor's view of IT risk and compliance across the IT enterprise</li> <li>Ingests and holds millions of data points from sensors to ease the burden on IT security personnel for sensor sample requests</li> <li>Automates the delivery of data samples to standard GRC tools and other reporting packages to ease the burden on IT security of audit requests</li> <li>Assessment and documentation of audit requirements to prepare for outside audits</li> </ul>



### 3. Continuous control over complex multi-cloud and hybrid environments.

As financial institutions continue with digital transformation, it's essential that their IT risk management platform support the compliance of on-premises, hybrid, cloud, and multi-cloud environments. Xacta integrates with leading cloud providers such as AWS and Microsoft Azure to simplify and streamline cloud compliance.

With Xacta, your workloads inherit pre-vetted security controls from your cloud hosts to simplify your audit of the compliance posture of cloud assets. Xacta also supports ongoing risk management and security validation in the

cloud to meet the continuous monitoring requirements of the leading standards and frameworks. These capabilities – unique to Xacta – result in 90 percent time savings in compliance level-of-effort to help you achieve continuous audit readiness.

**Xacta: 90 percent**  
time-savings in compliance and audit tasks – on-premises, in the cloud, and in hybrid / multi-cloud environments.

## Financial institutions require a dedicated, enterprise IT risk management solution. Make yours Xacta for fast, efficient cybersecurity audits.

Financial services organizations need to meet compliance requirements imposed by audits, but they can do so much more with the right ITRM solution. With automation, they can reduce the number of working days their security teams spend managing the audit process, re-deploy security and audit personnel to manage strategic tasks, free up budget to invest in growth, and innovate without the risk of falling out of compliance.

Xacta reveals risk in real-time and delivers proof of compliance with all major financial security standards for all types of environments—cloud, on-prem, and hybrid. With automated cyber risk management, you can speed time to compliance, saving time and effort for less-than-a-year ROI and ongoing support for emerging requirements.

For more information, please contact us.



Ken Michaels  
[ken.michaels@kttechnologies.net](mailto:ken.michaels@kttechnologies.net)  
<https://www.kttechnologies.net>

publication number: 5690-0628-B

