

## Tevora's Unified Assessment Program

THE ANTIDOTE FOR AUDIT FATIGUE

**M**aintaining compliance with the complex and sometimes overwhelming array of industry and government security requirements presents a daunting and resource-intensive challenge for many organizations. It's likely that many of your staff are experiencing the all-too-common "audit fatigue" as they are asked to support audit and certification efforts for multiple, often overlapping, security standards and frameworks each year.

The good news is that Tevora's proven Unified Assessment Program uses a methodology that reduces staff time required in support of audit and compliance efforts by an average of 55%. This significantly reduces audit fatigue and frees up time for staff to focus on strategic projects and other BAU activities. We accomplish this by taking a broad view of all security requirements an organization needs to comply with and leveraging this comprehensive perspective to develop an efficient and effective compliance strategy.

**Once the unified framework strategy is in place, we partner with clients to develop and implement compliance plans that eliminate redundant efforts, minimize staff time required, reduce costs, and provide clear and concise reporting that enables stakeholders to easily monitor progress.**

In this case study, we'll describe how Tevora used its Unified Assessment Program to help one of the world's leading communication services companies to stay compliant with a long list of security standards and frameworks while minimizing audit fatigue and costs. To protect our client's confidentiality, we'll refer to them by the fictitious name of Trans Global Communications (TGC).

# Struggling Under the Weight of Multiple Complex Compliance Requirements



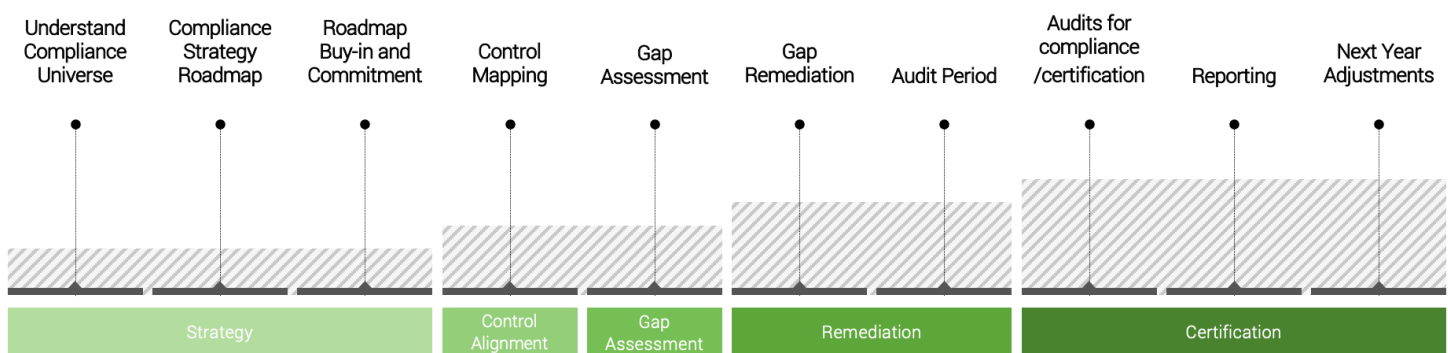
Tevora first began working with TGC eight years ago. At that time, they were struggling to comply with many complex and overlapping industry and government security standards, which was causing audit fatigue and high compliance costs.

They also had unique compliance challenges associated with their high-availability content delivery network that supports caching and streaming of data, audio, and video content. Any security enhancements or compliance testing in this environment had to be done without negatively impacting network latency, which was, and continues to be, a foundational requirement for their business.

# ► Understanding the Environment

After identifying the key TGC stakeholders, we held a kickoff meeting to introduce ourselves and discuss the unified security management approach we recommended for addressing their challenges. As part of this, we reviewed the five phases of our Tevora Unified Assessment Methodology. Here's a summary of the phases and milestones in each phase:

## Tevora Unified Assessment Methodology Phases and Milestones



We also reviewed the deliverables resulting from each phase of the methodology:

**STRATEGY PHASE**— Presentation outlining applicable frameworks, business units, products, stakeholders, audit approach, and proposed key dates/milestones.

**CONTROL & SCOPE ALIGNMENT PHASE**— Mapping across frameworks presented in an Excel workbook. Mapping will identify policy, procedure, and control alignment. In this mapping, we identify overlap for each control as partial, full, or none as well as identify possible further alignment to aid TGC's control activities.

**GAP ASSESSMENT PHASE**— Document presented in an Excel workbook with all mapped, applicable control gaps across frameworks with detailed remediation recommendations.

**REMEDIATION PHASE**— Policy templates, procedure examples, remediation facilitation documentation and verification, etc.

**CERTIFICATION PHASE**— Audit reports varying by framework and next year adjustments summary.

After reviewing the Unified Assessment Methodology, we conducted a series of follow up meetings with individual stakeholders to gain a detailed understanding of TGC's environment, challenges, and compliance requirements.

# ▶ Developing a Compliance Strategy Roadmap


After meeting with key stakeholders individually, we determined that TGC needed to be compliant with the following security standards and frameworks:

- ▶ International Standards Organization 27001, Information Security Management (ISO 27001)
- ▶ International Standards Organization 27701, Privacy Information Management System (ISO 27701)
- ▶ System and Organization Control (SOC) 2 Type 2
- ▶ Security Trust Assurance and Risk (STAR) Program
- ▶ Federal Information Security Modernization Act (FISMA)
- ▶ Payment Card Industry Data Security Standard (PCI DSS)
- ▶ Motion Picture Association of America (MPAA)
- ▶ Health Insurance Portability and Accountability Act (HIPAA)
- ▶ Health Information Trust Alliance (HITRUST)



Next, we worked with the TGC team to develop a compliance strategy roadmap for achieving compliance with, or re-certifying for compliance with, each of these frameworks or standards, using our Unified Assessment Methodology as a guide.

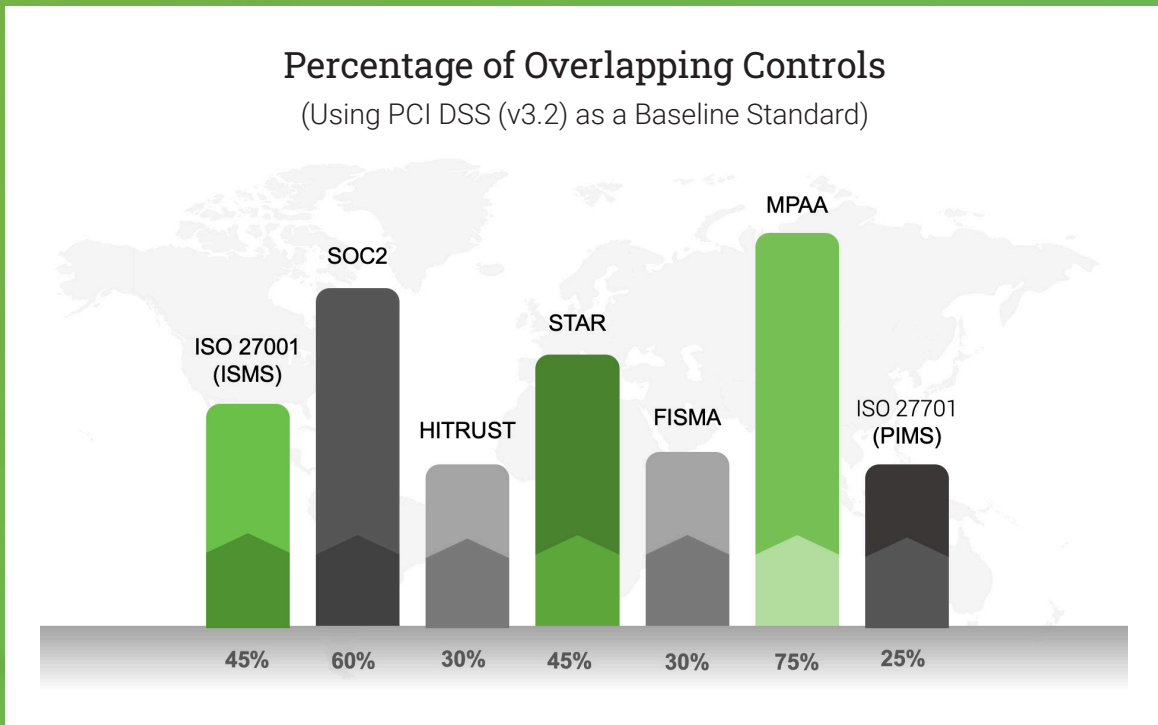
# Benefits



Taking a comprehensive view of TGC's compliance requirements and using a 12-month planning horizon enabled us to develop a compliance strategy that simplified and optimized the overall certification process and yielded significant benefits, including:

- ▶ **Reduced burden of staff interviews.** By identifying and grouping the requirements and interview topics that are common across multiple security standards and frameworks, we were able to substantially reduce the frequency and duration of staff interviews. We also spread interviews out over time to avoid bombarding team members with multiple interview requests at once. Our advanced planning allowed us to schedule interviews around peak periods when team members were involved in other key activities.
- ▶ **Streamlined testing and certification.** Common testing and certification requirements, test runs, and documentation were grouped to streamline testing, reduce sampling and documentation requests on TGC staff, and ultimately expedite the certification processes.

- ▶ **Synchronized controls and documentation.** We synchronized all common controls and documentation across the assessment teams and reports, which significantly reduced costs and staff time required. We also leveraged these commonalities to normalize control language across audits. The graphic below illustrates the high percentage of overlapping controls across different standards when PCI DSS version 3.2 is used as a baseline standard.



- ▶ **No impact on network latency.** By using a 12-month planning horizon, grouping common certification and testing activities, and staggering the timing of assessment phases for different standards and frameworks, we were able to spread out workloads and avoid overtaxing systems resources during periods of peak demand (e.g., major corporate events, peak systems demand timeframes, system maintenance/upgrade cycles). This approach allowed us to avoid any negative impact on network latency, which was an important requirement for TGC.
- ▶ **Fresh data and artifacts.** Our comprehensive, advanced planning process ensured “just-in-time” collection of data and artifacts needed for certification. This avoided the risk of poor certification results related to the use of stale data or artifacts.
- ▶ **Reduced audit fatigue.** In addition to improving operational efficiencies and reducing costs, one of the major benefits of our unified strategy and planning was a significant reduction in TGC’s audit fatigue.

## ▶ Diving Into Certification

After completing the Strategy phase and obtaining stakeholder buy-in for the Compliance Strategy Roadmap, Tevora's experienced team of security and compliance experts partnered with TGC staff to execute the remaining phases of the Unified Assessment Methodology (Control & Scope Alignment, Gap Assessment, Remediation, and Certification). This resulted in successful certifications for all of the security standards and frameworks that TGC wanted to comply with in the first year of our partnership.

One of the keys to success was having a TGC-assigned project manager that served as an internal champion for the effort, coordinated client activities, and worked in close partnership with the Tevora team to manage and report on every step of the process.

TGC management was thrilled with the cost reductions, improved efficiencies, successful certifications, and reduced audit fatigue that resulted from their partnership with Tevora in the first year. We also heard from many team members that our efforts had substantially relieved their audit fatigue, which improved their job satisfaction.

## ▶ Measurable Improvements

While it's always great to hear positive feedback from clients, we also feel it's important to quantify improvements whenever possible. Here are some of the key success metrics we captured for this project:

- ▶ 55% average reduction in staff time required in support of audit and compliance efforts
- ▶ 30% average reduction in TGC internal resource costs
- ▶ 10% average reduction in certification costs
- ▶ 100% increase in consistency of collected evidence
- ▶ 70% average increase in environment understanding of consulting team assigned (Tevora maintained consistency of the consulting team assigned to TGC where possible, or conducts internal knowledge transfers, so there was no need to re-explain everything to newly-assigned consultants)
- ▶ 60% average decrease in assessment/audit cycle period annually (audit time reduced from 12 months to 5 months)



# | Building On Success

Tevora has continued its strong partnership with TGC over the last eight years to maintain compliance with the initial set of security standards and frameworks as they evolve. We have also helped them comply with additional standards and frameworks over the years as they have expanded into new lines of business.

We continue to kick off the unified certification effort each year with a whiteboarding session in the first week of January, where we plan the upcoming year's activities.

As Tevora's knowledge of TGC's business, security, and compliance environments has deepened over time, we are increasingly asked to provide security services outside of the compliance domain and serve as advisors for many of their important business and technology initiatives.



# | Tevora Can Help



If you have questions about Tevora's Unified Assessment Methodology or would like help implementing it in your environment, Tevora's team of data privacy and security specialists can help. Just give us a call at [\(833\)292-1609](tel:8332921609) or email us at [sales@tevora.com](mailto:sales@tevora.com)