



**Teleperformance**

# Managing Security Risks in the Contact Center Business

**Bruce Wignall**  
**Chief Information Security Officer**





## **Table of Contents**

<b>Executive Summary</b>	<b>2</b>
<b>Contact Center Security Challenges</b>	<b>2</b>
<b>Trying to Build for What you Don't Know</b>	<b>2</b>
<b>The Teleperformance Security Framework</b>	<b>2</b>
<b>It takes a Partnership to Complete the Security Framework</b>	<b>2</b>
<b>Suggestions</b>	<b>2</b>



## Executive Summary

One of the greatest challenges for any organization today is providing adequate security to protect the confidentiality, integrity and availability of business data. This is no easy task for any company, even when that company is focused on a single business vertical such as health care.

On the surface, the contact center outsourcing industry is focused on providing customer management services for our clients. In reality, contact center outsourcers must operate and provide world class security controls for all the vertical industries and customer applications within which our clients operate.

This white paper considers the essential security elements for all vertical industries, and represents the leading standard for supporting these elements in the contact center outsourcing industry.

All businesses in every industry are challenged with the daunting task of balancing business functions and customer requirements with the confidentiality, integrity and availability of business data. Fortunately, frameworks in the

form of compliance or legal requirements that are intended to avoid breaches of any law, statutory, regulatory or contractual obligations are available for many of these industries.

For example, frameworks exist in the commerce and retail verticals for processing credit card transactions. This framework is called the Payment Card Industry standard or PCI.

Likewise, the healthcare industry follows the standards outlined by the

Health Insurance Portability and Accountability Act (HIPAA) of 1996. There are various other guidelines ranging from Senate Bill 1386 in California to the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada.

In addition to formal vertical regulations, there are many best practice compliance standards and strategies available as guidance to IT organizations. With ISO 17799, ISO 27001, COBIT, ITIL and various other strategies to follow, the task of security can appear daunting.

The contact center outsourcing industry has an obligation to extend its clients' regulatory or statutory requirements across the

partnership. In short, the service we provide exists as an extension of the services our clients provide.

With all the complexity and confusion demands centered on IT security, it's not unusual for organizations to perform the minimum tasks necessary to achieve regulatory or statutory compliance. We disagree with this approach because the regulatory or statutory regulations are intended to protect both the individual as well as the survivability of the business. Teleperformance believes that by complying entirely with these regulations and statutory requirements, we are demonstrating our leadership in our industry.

At Teleperformance, we view the major regulations, statutory obligations, regional requirements, and best practices as significant contributors to a superior security framework. We continually refine our services to fully support these requirements.

Teleperformance believes IT security will evolve to an international security language that will eventually meet the requirements for all security verticals. Until then, we support each major vertical regulatory or statutory requirement such as but



not limited to; HIPAA for health care, PCI for credit card transactions, regional requirements such as Senate Bill 1386 in California and PIPEDA in Canada and best practices such as ISO 17799, 27001 and ITIL.

Upon further reading of this article, you will understand how Teleperformance is specifically addressing these major considerations and why we are at the forefront at defining the future security standards for our entire industry.

### **Contact Center Security Challenges**

Most organizations operate within a single vertical market such as health care or telecommunications. These organizations must fulfill statutory or regulatory compliance associated with the vertical they operate within. In the case of health care, HIPAA and SOX are likely to be the two main compliance or statutory obligations. Achieving HIPAA and SOX compliance in and of itself is a major undertaking.

Now imagine the challenges the contact center industry is faced with. On the surface, the contact center industry may be viewed as a single vertical - the "contact center vertical". However, the reality is contact centers operate across all client vertical industries..

For instance, if a contact centers customer is in the health care industry, then HIPAA compliance requirements are extended to the contact center service provider. Contact centers that service clients in multiple industries are faced with every imaginable security statutory or regulatory compliance requirement. When you add multiple geographies into the mix, there are even more complexities.

Until recently, Information Security has not been tightly regulated. Non-compliance has not typically been associated with serious consequence. We are beginning to see that change. PCI "Payment Card Industry" not only requires annual investments to maintain certification, it also defines serious penalties for non-compliance up to and including the exclusion from operating as a service provider within the vertical.

In summary, contact centers have the complex responsibility to comply with the security requirements related to the vertical of their clients.

Other security challenges for the contact center industry include dealing with globalization and maintaining security requirements when offshoring.

### **Trying to Build for What you Don't Know**

The idea of multiple regulations or compliance frameworks is an indication of the immaturity of information security practices throughout the world. One would think you could follow a single strategy that will assure your compliance in multiple verticals. While this is not the case today, we expect to see an internal security language in the future.

Our security practice is built upon the strengths of the available security regulations or compliance frameworks available today. However, Teleperformance believes our strategy will closely resemble the likely future single international security language framework.

Unlike many companies, Teleperformance is not waiting to be told what to do. – We are marching forward and building what we feel is the security framework of the future. We are tailoring our security practice to comply with future statutory or regulatory frameworks as they are defined and even before they are fully established.

## The Teleperformance Security Framework

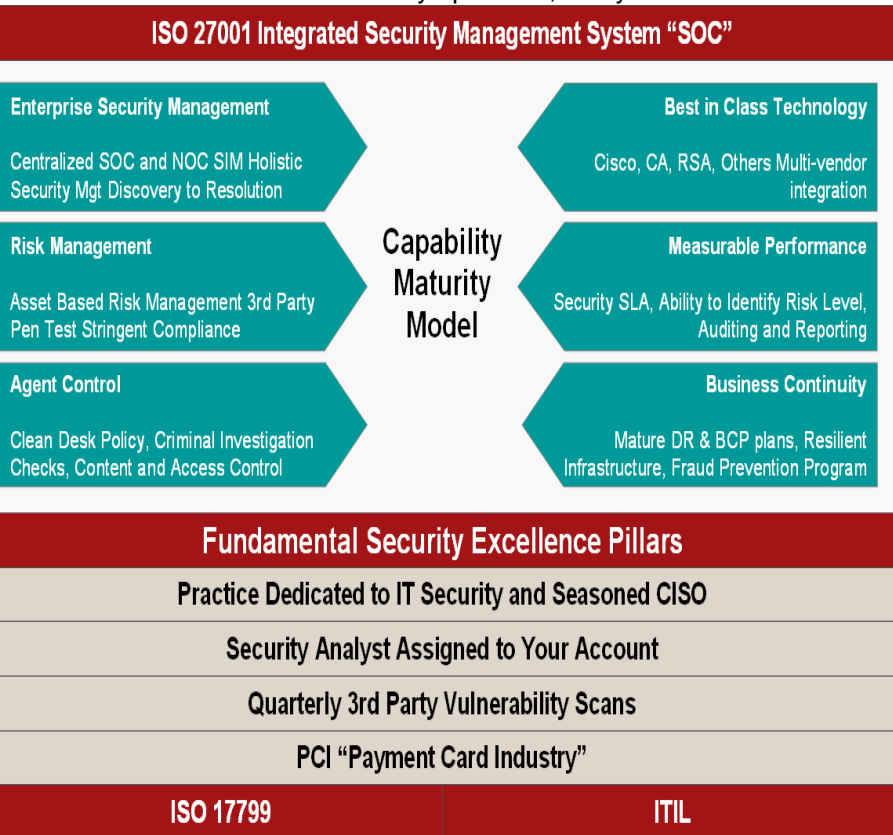
The following is an overview of the Teleperformance Security Framework. Our framework begins with compliance to a guideline for excellence in IT service. We have selected ITIL as our foundation for superior IT service. While we are not an IT only operation, many of our backend services

are highly dependent upon the underlying IT services. Without a single security framework or “universal security language” to follow, we decided to blend together multiple standards & processes to begin building a framework that will resemble a future universal security language (or framework).

Our business is that of both a service provider and an extension of your business. As an extension of your business, we enhance security by building it into all phases of services rather than bolting it on later as an afterthought.

Our security foundation begins with ISO17799 compliance. We selected ISO 17799 because it is an international security standard that can be used as the cornerstone of our security practice with the ability to add additional controls as needed for specific regulatory or statutory requirements.

Teleperformance understands that even bullet proof security



measures are subject to failure by poorly controlled and administered IT processes or procedures. We believe the best and most efficient IT shops share some common characteristics including:

- High service levels and availability
- Low amounts of unplanned work
- High success rates of change
- High investment early in the IT lifecycle
- Early and consistent process integration between IT operations and IT security
- High supportive posture of regulatory and statutory compliance
- Highly efficient system and network administration

Our desire to improve IT maturity and acquire these common characteristics lead us to the adoption of ITIL as a best practice or methodology.

Together ISO 17799 and ITIL provide the foundation layer that supports the other elements of our security architecture.

Next, we identified a framework that actually has some teeth for non-compliance. This is where we added the PCI “payment card industry” framework to our security foundation. Another reason for picking the PCI frame is simply because we want to include guidance from larger bodies of security professionals.

By adhering to PCI compliance, Teleperformance is required to conduct PCI security assessments annually. These annual assessment are required to be conducted by certified PCI 3rd party consulting firms. PCI compliance also requires quarterly 3rd party vulnerability scans. In short, both 3rd party requirements allow us to identify weaknesses or areas for improvement that we may have missed on our own.

**“Tevora has enjoyed the opportunity as a business partner to provide security services for Teleperformance. Teleperformance has a clear understanding of what it takes to provide a secure environment in the Contact Center industry. The security practice they are building has all the right elements to maintain confidentiality, integrity and availability to those companies who outsource their services to Teleperformance.”**

**Ray Zadjmool, CEO**



Now imagine a matrix that combines ITIL, ISO 17799 and the 3rd party scans and assessments. With this type of framework, we are able to demonstrate compliance with any regulatory or statutory requirement. Complying with other regulatory or statutory requirements now becomes an exercise in mapping requirements in our security practice with the requirements in other regulatory or statutory requirements.

It is simply a matter of “connecting the dots” to other regulatory or statutory requirements such as HIPAA for Health Care, SB1386 for California residents or PIPEDA for Canadian companies. We can prove our compliance to these other frameworks simply because their unique requirements are covered within our foundation security matrix of ITIL, ISO and 3rd party scans and vulnerability assessments.

Teleperformance realizes that understanding your business security needs is the next logical step in our security practice. That is why, in addition to other project and account management resources, you will be assigned a Security Analyst (SA). It is the responsibility of the SA to get close to your business and understand your unique security requirements. Teleperformance knows each of our clients have individual security requirements and we respond accordingly.

Once the SA understands your requirements, he/she will implement and manage the security aspects of your account throughout the life of the Teleperformance/client relationship.

Your Teleperformance SA is responsible for conducting regular reviews of the security service and managing to the security service level agreements “SLA”. The proactive nature of the SA’s role should reduce your time and effort traditionally needed to perform security audits.

The role of our CISO is to continuously identify better ways to improve the security services we offer. With Security Analysts as direct reports to the CISO, the communication from the client to is immediate and efficient.

By now, we hope you agree our security approach, principles and actual foundation is solid so, we will now focus on security technology and deliverables.

Below are a few examples of preferred vendor partners, processes, and deliverables within our security practice.

Use of best in class security technologies from companies like Cisco, RSA, PGP, CA and various others

Measurable performance – SLAs

Mature Disaster Recovery and Business Continuity procedures

NOC/SOC Command Center with proactive visibility down to the health and well being of each individual client’s environment

Risk management – based on real time asset based vulnerability management. We can identify in real time the known vulnerability level of every asset within the organization and the remediation steps

Strong agent controls beginning with background checks to clean desk polices and strong supervision

You should also know we have a solid overall process to support our multi-layered security framework. Teleperformance adheres to

ISO 27001 for best practices in security event and process management.



### **It takes a Partnership to Complete the Security Framework**

Even though we pride ourselves on the advances we have made in our security practices, we believe additional measures are required.

Regardless of whether you outsource contact center services or keep them in house, the possibility of agent fraud exists. That's why the investment in our partnership must include the sharing of appropriate reports or data for auditing purposes for both parties. Also, efficiencies between both parties must be maintained to insure latency in process or procedures do not create fraud opportunities.

An example of this includes the responsibility of Teleperformance to notify the customer of terminated employees and the responsibility of the customer to disable the terminated employee account in a timely manner. Another example of improved partnership is limiting the fraud potential of time by "federating" customer system access.

We are committed to proving you with superior security so that your security is not degraded at the point of outsource".

These are just a few examples of the investments Teleperformance believes must be made in our partnership with you. Without proper partnership investments in security, it is not a matter of "if" breakdowns will occur, but rather, "when" and "how bad" they will be.

### **Suggestions**

We believe the security practice at Teleperformance has already matured into what other companies hope to achieve in the future. We pride ourselves on our accomplishments but we understand of course, there is always room for improvement.

Your input or suggestions on improving our security practice is not only welcomed, but encouraged. We hope that you will take the time to provide us with your suggestions or comments on further improving our security practice.

Please contact Bruce Wignall with your suggestions, questions or comments:

[Bruce.Wignall@teleperformance.com](mailto:Bruce.Wignall@teleperformance.com)

Sincerely,

**Bruce Wignall CISSP**

**Chief Information Security Officer**

**Teleperformance Group International**