Armour Cybersecurity Case Study

NOTE: CLEINT DETAILS ARE KEPT CONFIDENTIAL DUE TO THE NATURE OF OUR WORK

# Global E-learning firm chooses Armour Cybersecurity to advise on Governance, Risk Management, and Compliance (GRC) practices in order to implement risk-based controls and prepare for an ISO 27001 certification.

Industry

*Education, E-learning and training with large enterprise clients.*

Challenge

*Client decided to pursue ISO 27001 certification. In-house security team was lacking necessary skill-set and capacity to take on the initiative.*

Results

*Armour Cybersecurity led the process from assessment, through implementation, to documentation through certification. Client passed ISO 27001 audit with flying colors.*

Key Benefits

- *Reduced business risk derived from cyber threat.*
- *ISO 27001certification was leveraged as a competitive advantage to win and secure additional business against competitors.*

## Overview

Our client is a global training and e-learning firm. Its main product is a platform that allows enterprise' training teams to create engaging learning environments for applications. The firm enables their cliental to easily onboard new employees, deepen user adoption, expedite application roll-outs, and maximize digital transformations. All at speed and at scale.

Our client provides services for large enterprise such as: Pepsi, Toyota, BNP Paribas, Philips, and others.

## Business Challenge

Given the nature of its work, our client is exposed to and hosting proprietary and confidential information for customers on its own platform. As such, its business risk exposure from cyber related threats needed to be tightened up around people, processes,

and technology. It also needed to address gaps created by operating in multiple regions with varying regulatory requirements and some highly regulated client environments. While our customer has had experience and in-house resources dedicated to cybersecurity, it was lacking in internal expertise in preparing the organization for an ISO 27001 audit.

## Why Armour Cybersecurity?

We were recommended to this client by another organization we have done similar work for. According to our client, it was "Armour's unique approach that allowed us to trust their process to deliver results in the aggressive timeline we have established."

Armour Cybersecurity has a very structured approach towards GRC projects. We envelop each line of business, understand its underlying objectives, identify sensitive and critical assets. With that in mind, we analyze unique and shared implications for departments and the organization as a whole. We then methodically assess the underlying findings and contrast those with best practices for good governance and risk management. Our diverse experience in managing cyber risk and compliance allows us to quickly identify gaps and areas of concern in order to set and implement cyber-control frameworks. By offering a range of cybersecurity services and technologies we can extend these to our clients. In this case, we have leveraged our capabilities to assist the client reach certification status under an aggressive timeline without loss of productivity on their side.

## The Plan

Understanding the customer objectives, risk appetite, and current security posture is critical to define and tailor cyber risk-based outcomes. In this case, our client, a mid-size company, needed to upgrade its security posture to enterprise level. The plan included deploying highly skilled resources leveraging Armour's mature methodologies and engaging our hands-on implantation team in an agile way as subsections were checked off.

## The Result

Using this plan, we were able to move our client to a pre-audit readiness phase quickly.  What usually takes months has taken weeks in this case, with a minimal business interruption.  Our client passed the ISO 27001 audit with flying colors. Beyond the need to comply with its own clients' requirements our client's determination to improve its cybersecurity posture was the belief "that it is the right thing to do" given the increasing amount of cyber attacks on supply chains. "Apart from our responsibility to our stakeholders, it also aligned with our goal to increase market share. We have leveraged our security work to gain more business against competitors".

Armour Cybersecurity protects organizations and their data from multi-faceted and ever-changing cyber threats. We provide end-to-end cybersecurity services backed by top global talent and a comprehensive ecosystem of leading technologies.

Our team boasts military backgrounds and many years of experience in cyber warfare & defense. We serve a variety of clients ranging from multi-billion-dollar, multinational corporations to small & medium-size businesses. We operate across a wide array of industries and geographies.

E: info@armourcyber.io

T:  1 866 80 30 700

W: armourcyber.io