KnowBe4

# **The Definitive Guide** to How Security Awareness Training Addresses Regulatory Compliance, Cyber Insurance and Security Frameworks

# The Definitive Guide to How Security Awareness Training Addresses Regulatory Compliance, Cyber Insurance and Security Frameworks

## Table of Contents

# INTRODUCTION

Chief information security officers (CISO) and security leaders now find themselves sitting in the middle of a three-way intersection where regulatory compliance, cyber insurance and security frameworks converge. In an environment where organization's and executives are being held accountable by government agencies, and even justice departments, for cyber attacks and data breaches, the role of security leadership has never been more critical—or complex.

What has emerged from this high-stakes environment is the increasing importance of security awareness training (SAT). Governments, regulatory bodies and insurance providers have all officially recognized that the weakest link in security is often the human element. They now expect organizations to address this through continuous education and assessments. Organizations that don't can be held accountable. Legally, the protection of sensitive data has extended beyond network defenses, firewalls and encryption tools and now encompasses a vigilant workforce.

SAT has officially transitioned from a cornerstone of an organization's cybersecurity program to a critical component that intersects with compliance, insurance and security frameworks. By embedding a culture of security awareness, organizations can enhance their compliance posture, improve their insurability and ensure that their security framework implementations are genuinely effective.

This eBook provides an overview of the role that SAT now plays across all three, in addition to outlining the major regulations and security frameworks that either mandate SAT or strongly encourage employee cybersecurity training.

> **"Governments, regulatory bodies and insurance providers have all officially recognized that the weakest link in security is often the human element."**


# REGULATORY COMPLIANCE AND SAT

As cyber threats grow in frequency and complexity, governments and regulatory bodies worldwide have responded by tightening the requirements for cybersecurity and data protection. A common denominator across nearly all major regulatory frameworks is the implementation of comprehensive SAT programs.

SAT has become a cornerstone of regulatory compliance. It is not merely a best practice but a mandated requirement across numerous global regulations. From the U.S. to Europe to Asia and the Middle East, regulatory frameworks such as FedRAMP, the Gramm-Leach-Bliley Act (GLBA), the Federal Information Security Modernization Act (FISMA), the General Data Protection Regulation (GDPR), the Network and Information Systems (NIS) Directive, the Cybersecurity Act, China's Cybersecurity Law (CSL), and the Personal Information Protection Law (PIPL) all emphasize the critical role that employee awareness and education play in safeguarding sensitive data and ensuring organizational security.

At the heart of these regulations lies a common understanding: despite advancements in technology and automated defenses, employees are frequently targeted by cybercriminals as a point of entry into an organization's systems. Phishing emails, social engineering attacks and other tactics that exploit human behavior can easily bypass even the most sophisticated technical defenses. As such, regulators have recognized that a well-trained workforce is crucial to mitigating these risks and ensuring compliance with data protection and cybersecurity standards.

As regulatory requirements continue to evolve, the importance of SAT cannot be overstated. It serves as a fundamental pillar of an organization's defense strategy, bridging the gap between technical safeguards and human behavior. By investing in comprehensive and continuous training programs, organizations not only ensure compliance with global regulations but also build a security-conscious culture.

This section outlines the major regulatory frameworks that either explicitly mandate SAT or strongly encourage employee cybersecurity training across:

- Global regulations
- North America
- Europe
- Africa
- Asia
- South America
- Middle East

This is not intended as a comprehensive list, but rather an overview of key regional and/or national regulations that organizations should use as a starting point when evaluating SAT within the context of regulatory compliance.

## Global Regulations

Several cybersecurity and data protection regulations have a global impact, either because they directly apply to organizations operating across multiple continents or because they have extraterritorial provisions that affect companies worldwide. These regulations often mandate SAT as part of broader compliance requirements. Here are the key global regulations:

| | | |
|---|---|---|
| **General Data Protection Regulation (GDPR)** | Region: Primarily European Union (EU), but with global impact | Applies to any organization, regardless of location, that processes the personal data of individuals within the EU.<br><br>GDPR requires organizations to ensure that employees are adequately trained in data protection principles. This includes understanding how to handle personal data, recognizing data breaches and complying with data subject rights. Training is considered essential for maintaining compliance and preventing breaches. |
| **Payment Card Industry Data Security Standard (PCI DSS)** | Region: Global | Applies to any organization that processes, stores or transmits credit card information. PCI DSS mandates that organizations implement SAT for all personnel. This training must cover data security practices, the importance of protecting cardholder data and recognizing potential security threats. Regular training is required to maintain compliance with the standard. |
| **Health Insurance Portability and Accountability Act (HIPAA)** | Region: Primarily the United States, but affects global entities handling U.S. healthcare data. | Applies to healthcare providers, health plans and business associates that handle Protected Health Information (PHI) in the U.S.<br><br>HIPAA mandates that organizations provide SAT to all employees, covering topics such as data privacy, security risks and compliance with HIPAA rules. Organizations with global operations that handle U.S. healthcare data must ensure their employees are trained according to HIPAA standards. |
| **Gramm-Leach-Bliley Act (GLBA)** | Region: Primarily the United States, with global implications for multinational financial institutions. | Applies to financial institutions operating in the U.S. GLBA requires financial institutions to develop a comprehensive information security program that includes SAT for employees. The training should focus on safeguarding customer information and complying with privacy and data protection rules. Global financial institutions must ensure compliance with GLBA even if they operate outside the U.S. |

| | | |
|---|---|---|
| **Federal Risk and Authorization Management Program (FedRAMP)** | Region: Primarily the United States, but impacts global cloud service providers offering services to U.S. federal agencies. | Applies to cloud service providers (CSPs) that want to sell services to the U.S. federal government. FedRAMP requires CSPs to implement SAT for all personnel as part of their security program. This training must address the specific security requirements for handling federal data and ensure that employees are equipped to recognize and respond to cyber threats. |
| **Network and Information Systems (NIS) Directive** | Region: European Union, with global impact on critical infrastructure and digital service providers. | Applies to operators of essential services and digital service providers within the EU. The NIS Directive mandates that organizations implement security measures, including training employees on cybersecurity risks and incident response procedures. Companies outside the EU that provide critical services within the EU may also be subject to these requirements. |
| **Cybersecurity Act (EU)** | Region: European Union, with global implications for products and services marketed in the EU. | Establishes a framework for cybersecurity certification of products, processes and services. Although primarily focused on certification, the Cybersecurity Act emphasizes the importance of cybersecurity awareness and training as part of maintaining certified security practices. This indirectly requires organizations to ensure their personnel are trained in cybersecurity. |
| **China's Cybersecurity Law (CSL)** | Region: Primarily China, but with global impact on companies doing business in China. | Applies to organizations operating in China, particularly those handling Chinese citizens' personal data or operating critical information infrastructure.<br><br>CSL mandates that organizations provide cybersecurity training and education to their employees to protect personal data and national security. Multinational companies with operations in China must comply with these requirements. |
| **Personal Information Protection Law (PIPL)** | Region: Primarily China, but with extraterritorial reach affecting global companies processing Chinese citizens' data. | Applies to any entity processing the personal data of Chinese citizens, regardless of where the entity is located. PIPL requires organizations to train employees on data protection practices, ensuring they understand their obligations under the law. Training is essential to prevent breaches and ensure compliance with China's stringent data protection regulations. |

| | | |
|---|---|---|
| **European Union Artificial Intelligence Act (EU AI Act)** | Region: While the Act applies within the EU, its stringent standards are expected to have global implications, as companies worldwide that wish to operate in the EU or offer AI-related products and services there will need to comply with its provisions. | The EU AI Act is a comprehensive regulatory framework designed to govern the development, deployment and use of artificial intelligence within the European Union. It focuses on high-risk AI systems to ensure they are safe, transparent and respect fundamental rights. The Act mandates that for high-risk AI systems, appropriate human oversight must be ensured to prevent or minimize the risks to health, safety or fundamental rights. This includes training human operators to understand the AI system's capabilities and limitations, and to intervene if necessary. The goal is to prevent over-reliance on AI and to ensure that humans remain in control of critical decisions. (refer to Title III, Chapter 2, Article 14) |

## North America

In North America, several cybersecurity regulations mandate SAT as a critical component of compliance. These regulations often aim to protect sensitive information, ensure data privacy and mitigate cyber risks. Here are the major regulations:

| United States | |
|---|---|
| **Federal Information Security Modernization Act (FISMA)** | Impacts federal agencies and their contractors. Requires regular training on security awareness and specific role-based training to protect federal information systems. |
| **New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500)** | Applies to financial institutions operating in New York State. Requires a cybersecurity program, including a SAT program for all personnel. |
| **California Consumer Privacy Act (CCPA)** | Impacts companies doing business in California that meet certain criteria (e.g., revenue thresholds, data collection volumes). While not explicitly mandating training, it implies the need for employee awareness to handle consumer data properly. |
| **Canada** | |
| **Personal Information Protection and Electronic Documents Act (PIPEDA)** | Impacts private sector organizations handling personal information. While PIPEDA does not explicitly mandate SAT, it necessitates safeguarding personal information, which often includes training as a best practice. |
| **Provincial Legislation** | Impacts various industries across different provinces, such as the Freedom of Information and Protection of Privacy Act (FIPPA) in Ontario and British Columbia. Similar to PIPEDA, these laws require reasonable measures to protect personal information, often including employee training. |
| **Canada's Anti-Spam Legislation (CASL)** | Applies to all organizations sending commercial electronic messages. Training is often part of compliance to ensure employees understand the rules and restrictions on electronic communications. |

| Mexico | |
|---|---|
| **Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP)** | Impacts private organizations handling personal data. Requires organizations to implement training programs for employees to ensure proper data protection practices. |

## Europe

In Europe, several regulations and frameworks mandate or strongly encourage organizations to implement SAT. Here are the major regulations:

| | |
|---|---|
| **ePrivacy Directive (Directive on Privacy and Electronic Communications)** | Impacts all organizations offering public electronic communications services or networks in the EU. While the ePrivacy Directive focuses on the confidentiality of communications and online privacy, organizations must ensure employees understand the regulations and how to handle personal data securely, typically through training. |
| **Payment Services Directive 2 (PSD2)** | Applies to payment service providers in the European Economic Area. PSD2 requires strong customer authentication and secure communication. Organizations must train employees on secure payment practices and the handling of sensitive payment data. |
| **European Banking Authority (EBA) Guidelines on ICT and Security Risk Management** | Applies to financial institutions within the EU. The guidelines require financial institutions to implement an information and communication technology (ICT) and security risk management framework. This includes ensuring that staff receive appropriate training on cybersecurity and ICT risks. |
| **Sector-Specific Regulations** | **Financial Sector:** The Basel Committee on Banking Supervision and the European Securities and Markets Authority (ESMA) provide guidelines that often emphasize the importance of training and awareness in managing cyber risks.<br><br>**Healthcare Sector:** Organizations must comply with the GDPR, and additional sector-specific regulations may require specific training on handling health data. |
| **National Regulations** | **Germany's IT Security Act:** Requires critical infrastructure operators to provide training to employees to ensure cybersecurity.<br><br>**UK's Data Protection Act 2018:** Aligns with GDPR but also emphasizes the need for organizations to ensure staff are trained and aware of data protection responsibilities. |

# Africa

In Africa, several countries have developed cybersecurity and data protection regulations that emphasize the importance of SAT. These regulations are designed to protect personal data and enhance cybersecurity across various sectors. Here's an overview of key regulations across the continent that include provisions for SAT:

| Africa | |
|---|---|
| **The Malabo Convention** | The Malabo Convention, officially known as the African Union Convention on Cyber Security and Personal Data Protection, is a legal framework adopted by the African Union in 2014. The convention aims to enhance cybersecurity, protect personal data and regulate electronic transactions across Africa. It encourages member states to criminalize cyber crime, establish data protection laws and create national authorities for cybersecurity and data protection enforcement. |
| **South Africa** | |
| **Protection of Personal Information Act (POPIA):** | Applies to the processing of personal information by public and private entities in South Africa. POPIA mandates that organizations implement appropriate security measures to protect personal data, which includes training employees on data protection principles and practices. The law emphasizes the need for organizations to ensure that staff are aware of their responsibilities regarding data privacy and security. |
| **National Cybersecurity Policy Framework (NCPF):** | Provides a comprehensive framework for cybersecurity governance in South Africa. The NCPF highlights the need for capacity building and education, including SAT for all stakeholders to improve the overall cybersecurity posture of the country. |
| **Kenya** | |
| **Data Protection Act, 2019** | Applies to the processing of personal data by both public and private entities in Kenya.<br><br>The law requires organizations to implement security measures, including regular training for employees on data protection and cybersecurity. The training ensures that employees understand the risks associated with data processing and are aware of how to protect personal data. |
| **Computer Misuse and Cybercrimes Act, 2018** | Addresses cyber crimes and cybersecurity measures in Kenya. The act mandates organizations to adopt cybersecurity measures, including educating and training employees to recognize and respond to cyber threats effectively. |
| **Nigeria** | |
| **Nigeria Data Protection Regulation (NDPR)** | Applies to the processing of personal data in Nigeria. The NDPR requires organizations to ensure that their employees are trained in data protection principles and practices. This includes raising awareness about the importance of data privacy and implementing security measures to protect personal data. Data security is outlined with specific controls that include "continuous capacity for building staff. |

| | |
|---|---|
| **Cybercrimes (Prohibition, Prevention, etc.) Act, 2015** | Governs cybersecurity and cyber crime prevention in Nigeria. The act mandates the implementation of security measures, including regular training and awareness programs for employees to mitigate cyber risks and ensure compliance with cybersecurity standards. |
| **Ghana** | |
| **Data Protection Act, 2012 (Act 843)** | Regulates the processing of personal data by public and private entities in Ghana. The law requires data controllers to implement security measures, including employee training on data protection and cybersecurity, to safeguard personal data and ensure compliance with data protection principles. |
| **Cybersecurity Act, 2020** | Establishes a comprehensive cybersecurity framework in Ghana. The act emphasizes the need for continuous capacity building, including SAT, to strengthen the country's cybersecurity posture and protect critical information infrastructure. |
| **Mauritius** | |
| **Data Protection Act 2017** | Applies to the processing of personal data in Mauritius. The act requires organizations to implement appropriate technical and organizational measures to protect personal data, which includes training employees on data protection principles and cybersecurity practices. |
| **Computer Misuse and Cybercrime Act 2003** | Addresses cyber crime and cybersecurity measures in Mauritius. The act highlights the importance of cybersecurity education and training to prevent cyber crimes and enhance the overall cybersecurity framework of the country. |
| **South Africa** | |
| **Protection of Personal Information Act (POPIA)** | POPIA is South Africa's equivalent of the GDPR, designed to protect the personal data of South African citizens. It governs how organizations collect, process, store, and share personal information. POPIA requires organizations to implement appropriate technical and organizational measures to prevent unauthorized access or data breaches. It also emphasizes the need for employee training on data protection and cybersecurity practices |
| **Cybercrimes Act (2020)** | The Cybercrimes Act was introduced to combat cybercrime more effectively and align South African law with international cybercrime frameworks and criminalizes cyber-related offenses such as hacking, ransomware, and identity theft. It also introduces measures for preventing, detecting and investigating cybercrime. |
| **National Cybersecurity Policy Framework (NCPF)** | The NCPF provides a broad policy for enhancing cybersecurity in South Africa. It emphasizes public-private cooperation to strengthen national cyber defenses and outlines steps to protect critical infrastructure and secure South Africa’s cyberspace. It also highlights the need for capacity building and cybersecurity awareness programs across sectors. |

| | |
|---|---|
| **King IV Report on Corporate Governance** | While not specific to cybersecurity, the King IV Report is a key governance framework in South Africa that promotes ethical and effective leadership in all areas of business, including IT governance and risk management, ensuring that cybersecurity risks are adequately managed. It promotes ongoing monitoring of cybersecurity controls and encourages fostering a security-conscious culture by holding senior leaders accountable for ensuring that cybersecurity is part of the overall business strategy. |
| **Tunisia** | |
| **Organic Law on the Protection of Personal Data (Law No. 2004-63)** | Applies to the processing of personal data in Tunisia. The law requires data controllers to implement security measures, including training employees on data protection practices to ensure compliance and safeguard personal data. |
| **Rwanda** | |
| **Law Governing Information and Communication Technologies (ICT Law)** | Covers the regulation of ICTs and cybersecurity in Rwanda. The law mandates organizations to adopt security measures, including regular training and awareness programs for employees, to protect against cyber threats and ensure the secure handling of information. |

## Asia

In Asia, various countries have implemented regulations and frameworks that either mandate or strongly encourage SAT as part of broader cybersecurity and data protection measures. Here are some key regulations across different Asian countries:

| | |
|---|---|
| **Japan** | |
| **Act on the Protection of Personal Information (APPI)** | Applies to entities handling personal information in Japan. APPI requires organizations to implement security measures, including educating employees on data protection and ensuring they are aware of their responsibilities regarding personal information. |
| **Cybersecurity Management Guidelines** | Applicable to organizations across various sectors. These guidelines, issued by Japan's Ministry of Economy, Trade, and Industry (METI), stress the importance of cybersecurity awareness and training for all employees as part of a comprehensive cybersecurity management system. |
| **South Korea** | |
| **Personal Information Protection Act (PIPA)** | Applies to all organizations handling personal information in South Korea. PIPA mandates organizations to implement measures to protect personal information, which includes regular SAT for employees to prevent data breaches and ensure compliance with data protection standards. |
| **Network Act** | Covers providers of information and communication services. This act requires organizations to protect users' personal information and maintain network security. Employee training on cybersecurity practices is a critical component of these requirements. |

| | |
|---|---|
| **Singapore** | |
| **Personal Data Protection Act (PDPA)** | Applies to all private sector organizations handling personal data in Singapore. The PDPA requires organizations to take steps to protect personal data, which includes training employees on data protection and security practices. |
| **Cybersecurity Act** | Focuses on operators of critical information infrastructure (CII) and cybersecurity service providers. The act mandates cybersecurity measures, including SAT for employees, to protect critical systems and data from cyber threats. |
| **India** | |
| **Information Technology Act, 2000 (IT Act)** | Applies to all entities engaged in digital transactions and data processing. The IT Act and its accompanying rules, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, emphasize the need for organizations to implement security measures. This includes training employees on cybersecurity best practices and data protection. |
| **Personal Data Protection Bill** | Once enacted, it will apply to all entities processing personal data of Indian residents. The draft bill outlines provisions for data protection, including the requirement for organizations to ensure that employees handling personal data are trained in data protection principles and practices. |
| **Hong Kong** | |
| **Personal Data (Privacy) Ordinance (PDPO)** | Applies to all entities handling personal data in Hong Kong. The PDPO mandates that organizations take reasonable precautions to protect personal data, which often includes training employees on data privacy and security. |
| **Thailand** | |
| **Personal Data Protection Act (PDPA)** | Impacts all organizations processing personal data in Thailand. The PDPA requires data controllers and processors to implement security measures, including employee training, to protect personal data and ensure compliance with the law. |
| **Malaysia** | |
| **Personal Data Protection Act (PDPA)** | Applies to private sector organizations handling personal data in Malaysia. The PDPA requires organizations to implement security measures to protect personal data, which includes training employees on data protection practices. |

## South America

In South America, various countries have enacted regulations to address data protection and cybersecurity, often requiring or encouraging SAT as part of broader compliance measures. Here are some notable regulations:

| | |
|---|---|
| **Brazil** | |
| **General Data Protection Law (Lei Geral de Proteção de Dados - LGPD)** | Applies to any individual or organization processing personal data in Brazil, regardless of where they are located. The LGPD mandates that organizations implement security measures to protect personal data, which includes training employees on data protection and security practices. The law emphasizes the importance of raising awareness about privacy and data protection principles among employees. |
| **Internet Act (Marco Civil da Internet):** | Impacts all internet service providers and users in Brazil. While not explicitly focusing on training, the law underscores the need for providers to implement security measures, which can include educating employees about cybersecurity best practices to protect user data. |
| **Argentina** | |
| **Personal Data Protection Law (Ley de Protección de los Datos Personales - Law No. 25,326):** | Applies to all entities handling personal data in Argentina. The law requires data controllers to adopt measures to ensure the security and confidentiality of personal data. This typically involves training employees who handle personal data to prevent unauthorized access or data breaches. |
| **Chile** | |
| **Personal Data Protection Law (Ley sobre Protección de la Vida Privada - Law No. 19,628):** | Applies to the processing of personal data by public and private entities in Chile. The law requires entities to take measures to protect personal data, which includes ensuring employees are trained in data protection and security practices. |
| **Colombia** | |
| **Statutory Law on Data Protection (Ley Estatutaria de Protección de Datos - Law No. 1581)** | Applicable to entities processing personal data in Colombia. The law mandates that organizations implement administrative, technical and physical measures to ensure data security, which often includes training employees on data protection principles and security measures. |
| **Cybersecurity and Cyberdefense Policy (Conpes Document 3701):** | Provides a framework for cybersecurity and cyberdefense in Colombia. The policy highlights the need for public and private entities to educate and train their workforce on cybersecurity risks and best practices. |
| **Peru** | |
| **Personal Data Protection Law (Ley de Protección de Datos Personales - Law No. 29733):** | Applies to the processing of personal data in Peru. The law requires organizations to implement security measures to protect personal data, including training employees on the proper handling and protection of data. |

| Uruguay | |
|---|---|
| **Personal Data Protection Law (Ley de Protección de Datos Personales - Law No. 18,331):** | Applies to the processing of personal data by public and private entities in Uruguay. The law mandates that organizations ensure the security and confidentiality of personal data, often involving employee training on data protection and security policies. |

## Middle East

In the Middle East, various countries have implemented regulations and guidelines to address data protection and cybersecurity. These regulations often include requirements for SAT as part of broader efforts to enhance organizational security and protect sensitive information. Here are some key regulations across the region:

| United Arab Emirates (UAE) | |
|---|---|
| **UAE Data Protection Law (Federal Decree-Law No. 45 of 2021):** | Applies to the processing of personal data within the UAE, excluding certain free zones. The law mandates that organizations implement adequate security measures to protect personal data, which includes providing training and awareness programs to employees on data protection and cybersecurity practices. |
| **Dubai International Financial Centre (DIFC) Data Protection Law (Law No. 5 of 2020):** | Applicable to the DIFC, an economic free zone in Dubai. Organizations are required to ensure that employees handling personal data are trained in data protection principles, as part of their responsibility to safeguard data security. |
| **Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021:** | Applies to the ADGM, an international financial center in Abu Dhabi. The regulations emphasize the importance of training employees on data protection and cybersecurity, particularly for those handling personal data. |
| **Saudi Arabia** | |
| **Personal Data Protection Law (PDPL):** | Applies to the processing of personal data within Saudi Arabia. The PDPL requires organizations to implement security measures to protect personal data, including regular training and awareness programs for employees to understand data protection and privacy obligations. |
| **Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework:** | Applies to financial institutions regulated by SAMA. The framework mandates that organizations provide cybersecurity training and awareness programs to all staff, particularly those in sensitive or critical roles. |
| **National Cybersecurity Authority (NCA) Essential Cybersecurity Controls:** | Applicable to government agencies and critical infrastructure organizations in Saudi Arabia. These controls require organizations to conduct regular SAT for employees to foster a security-conscious culture. |

| | |
|---|---|
| **Qatar** | |
| **Data Protection Law (Law No. 13 of 2016):** | Applies to the processing of personal data in Qatar. The law mandates that organizations implement appropriate security measures, including training employees on data protection and privacy practices. |
| **Qatar Financial Centre (QFC) Data Protection Regulations:** | Applies to entities within the QFC, a financial and business center. Organizations must provide training to employees handling personal data to ensure they understand their responsibilities under the data protection regulations. |
| **Bahrain** | |
| **Personal Data Protection Law (PDPL):** | Applies to the processing of personal data in Bahrain. The PDPL requires data controllers to take appropriate security measures, including providing training and awareness to staff on data protection principles and security measures. |
| **Israel** | |
| **Privacy Protection Regulations (Data Security), 2017:** | Applies to all organizations handling personal data in Israel. The regulations require organizations to conduct regular training and awareness programs for employees on data security measures and privacy laws. |
| **Oman** | |
| **Electronic Transactions Law (Royal Decree No. 69/2008)** | Governs electronic transactions and related activities in Oman. While the law emphasizes secure electronic transactions, it also highlights the need for organizations to educate employees about cybersecurity best practices. |
| **Oman Personal Data Protection Law (Royal Decree No. 6/2022)** | Applies to the processing of personal data in Oman. The law requires organizations to implement measures to protect personal data, which includes training employees on data protection and security practices. |
| **Kuwait** | |
| **E-Transactions Law (Law No. 20 of 2014):** | Regulates electronic transactions and data protection in Kuwait. The law emphasizes the importance of data security and mandates organizations to train employees on cybersecurity and data protection measures. |


# CYBER INSURANCE AND SAT

As the cost of cyber attacks and data breaches continues to grow, many organizations are turning to cyber insurance policies as a critical component of their risk management strategies.

According to the **2024 Cyber Claims Report**, the frequency of cyber claims has increased 13% year over year since 2021, and the average claim has increased by 10% over the same time period.

As a result, organizations are realizing that simply purchasing a policy is not enough. Insurers are placing greater emphasis on proactive measures, such as SAT, to assess and mitigate risk. Training helps lower an organization's risk profile, which can lead to more favorable terms and reduced premiums in cyber insurance policies.

Case in point, according to **Sophos' Cyber Insurance and Cyber Defense 2024** report, 97% of organizations plan on improving cyber defenses alongside obtaining a cyber insurance policy, with two-thirds of those organizations planning on making a "major" investment. These investments in defenses have a material impact on an organization's cyber insurance position:

- 76% of organizations were able to qualify for coverage
- 67% were able to obtain better coverage
- 30% were able to receive better pricing

There are four primary reasons that SAT positively impacts cyber insurance rates:

**1** **Reduced Risk Profile**
Insurance companies often assess an organization's overall risk posture when determining premiums. Organizations that invest in comprehensive SAT demonstrate a commitment to reducing risk, which can make them more attractive to insurers. For instance, if a company regularly conducts phishing simulations and provides ongoing training, it may be viewed as less likely to suffer from a phishing-related breach. This reduced risk can lead to lower insurance rates.

**2** **Meeting Underwriting Requirements**
Some cyber insurance policies have underwriting requirements that include evidence of employee training programs. For example, an insurer might require annual training on data protection and incident response as a condition for coverage. By meeting these requirements, organizations can qualify for more favorable policy terms, including lower premiums. A case in point is that companies with demonstrated adherence to security best practices, including regular training, are often eligible for discounts or lower deductibles.

**3** **Compliance with Industry Standards**
Insurance companies often offer reduced rates to organizations that comply with recognized industry standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or the ISO/IEC 27001 standard. SAT is a critical component of these standards, as it ensures that employees understand their roles in protecting sensitive information. Compliance with such standards can not only reduce premiums but also ensure better coverage terms.

**4** **Case Studies and Insurer Programs**
Certain insurers have explicitly stated that they offer premium reductions for clients who implement robust cybersecurity training programs. For example, some insurers provide discounts for companies that conduct regular employee training on topics like phishing, password management and safe internet practices. These programs are often part of a broader initiative to encourage better cybersecurity hygiene and reduce the likelihood of claims.

Generally speaking, an insurance company can offer between a **10-20% discount[1] on premiums** for organizations that can prove they've conducted comprehensive SAT in the past year. Insurers recognize that a well-informed and vigilant workforce is less likely to fall victim to cyber attacks, which ultimately reduces the insurer's potential liability.

1 Based on research by Forrester Research, Willis Towers Watson and KnowBe4


# SECURITY FRAMEWORKS AND SAT

As cyber threats become more sophisticated, security frameworks have evolved to address the growing need for comprehensive security strategies. Initially, these frameworks focused heavily on technical controls and processes, with less emphasis on the human factor. However, as organizations experience breaches caused by phishing, social engineering and insider threats, the importance of addressing the human element has become increasingly evident.

Frameworks such as NIST CSF, ISO/IEC 27001 and COBIT have gradually expanded their scope to include SAT as a core component. They recognize that even the most advanced technologies can be rendered ineffective if the people using them are not properly trained. Employees are often the first line of defense against cyber threats, and their ability to identify and respond to suspicious activities is crucial to the organization's overall security posture.

Despite this progress, the human element in cybersecurity is still not fully understood or appreciated. Security frameworks are beginning to acknowledge the complexity of human behavior and its impact on security, but there is still much to learn. Understanding the psychological and cultural factors that influence employee behavior, for instance, remains a challenge. As frameworks continue to develop, we can expect a deeper integration of human factors into cybersecurity strategies, emphasizing not only awareness but also behavior change, engagement and continuous education. This evolution will be essential in creating a more holistic approach to cybersecurity, where both technology and human elements work in tandem to protect organizations from emerging threats.

Here are seven of the most common security frameworks that have security awareness and compliance training as key requirements:

| | |
|---|---|
| **NIST**<br>**Cybersecurity Framework (NIST CSF)** | **Security Awareness Connection**: The framework includes the "Protect" function, which covers security training and awareness as part of the safeguards necessary to ensure the delivery of critical infrastructure services. |
| **ISO/IEC 27001** | **Security Awareness Connection**: Clause 7.2.2 requires that all employees of an organization are aware of the security policies and procedures relevant to their job responsibilities. The standard emphasizes the importance of training and awareness programs to ensure compliance with security policies. |
| **COBIT**<br>**(Control Objectives for Information and Related Technologies)** | **Security Awareness Connection**: COBIT includes management objectives for people, skills and competencies, emphasizing the need for security awareness and training to support IT governance and management. |

| | |
|---|---|
| **CIS Controls**<br>**(Center for Internet Security Controls)** | **Security Awareness Connection**: Control 17 focuses specifically on security awareness and skills training, recommending that organizations implement a security awareness program to promote a culture of security and educate users on safe practices. |
| **SOC 2**<br>**(Service Organization Control 2)** | **Security Awareness Connection**: Under the security trust service principle, SOC 2 emphasizes the need for SAT to ensure that employees understand their responsibilities and the importance of protecting client data. |
| **CMMC**<br>**(Cybersecurity Maturity Model Certification)** | **Security Awareness Connection**: CMMC includes specific practices related to SAT at various maturity levels. It emphasizes training for both general cybersecurity awareness and role-based training for specialized security functions. |
| **CSA CCM**<br>**(Cloud Security Alliance Cloud Controls Matrix)** | **Security Awareness Connection**: The CCM emphasizes the need for SAT to ensure that employees understand the security risks associated with cloud services and their role in mitigating those risks. |

# CONCLUSION

SAT is no longer just a regulatory requirement; it's a critical element in achieving compliance, securing favorable cyber insurance and effectively implementing security frameworks. By fostering a security-conscious workforce, organizations can better meet the demands of both global and local regulations, while also better aligning with influential information security frameworks. For security leaders, investing in continuous and comprehensive SAT is essential for building a resilient cyber defense that mitigates risks and enhances overall security posture.

Here are additional assets to understand what to look for when evaluating SAT platforms and how to build a security culture within your organization:

**Critical Considerations When Evaluating Security Awareness Training Vendors**

**Download Now**

**The Security Culture How-To Guide**

**Download Now**

## Additional Resources

**Free Phishing Security Test**
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

**Free Automated Security Awareness Program**
Create a customized Security Awareness Program for your organization

**Free Phish Alert Button**
Your employees now have a safe way to report phishing attacks with one click

**Free Email Exposure Check**
Find out which of your users emails are exposed before the bad guys do

**Free Domain Spoof Test**
Find out if hackers can spoof an email address of your own domain


## About KnowBe4

KnowBe4 empowers your workforce to make smarter security decisions every day. Tens of thousands of organizations worldwide trust the KnowBe4 platform to strengthen their security culture and reduce human risk. KnowBe4 builds a human layer of defense so organizations can fortify user behavior with new-school security awareness and compliance training.

Deploying KnowBe4 results in users that are alert and care about the damage that phishing, ransomware and other social engineering threats pose. The platform includes a comprehensive suite of awareness and compliance training, real-time user coaching, AI-powered simulated social engineering, and crowdsourced anti-phishing defense.

With content in 35+ languages, KnowBe4 provides the world's largest, always-fresh library of engaging content to strengthen your human firewall.

**For more information, please visit www.KnowBe4.com**

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com



01E10K01