MetaCompliance®

Security Awareness Training Roadmap

Make it personal.

metacompliance.com

Summary

This roadmap serves as a structured guide for developing and maintaining an effective Security Awareness Training program. It breaks down the process into three key phases: Preparation, Implementation, and Review & Enhancement. Each phase builds on the previous one, fostering a culture of continuous improvement that adapts to evolving security threats and organisational needs.

Phase 1 (Preparation):
Focus on planning, developing content, and ensuring leadership buy-in.

Phase 2 (Implementation):
Deliver training, engage employees, and track progress.

Phase 3 (Review & Enhancement):
Evaluate the program's effectiveness, make improvements, and reinforce key lessons.

Phase 1: Preparation

Conduct a Risk Assessment:

Start by conducting a risk assessment to identify the most relevant security risks to your organisation, such as phishing, malware, and social engineering threats. This assessment will guide the development of targeted training materials.

Define Training Objectives:

Training objectives should be defined in alignment with the organisation's security policies and compliance requirements. Setting specific learning outcomes ensures that the training program remains focused on addressing the key areas of concern.

Identify Target Audience:

It's essential to segment users and tailor the training to the specific needs of different groups within the organisation. Role-based training should be developed for employees, contractors, and executives, ensuring that each group receives relevant content that addresses their unique responsibilities.

Platform Preparation:

To deliver the training effectively, the organisation's chosen platform must be prepared. This involves customising the platform with your organisation's branding and ensuring that it supports tracking, reporting, and content updates. With the platform in place, the next step is to develop the training program itself.

Program Development:

Create a training program tailored to your goals, objectives, audience, and capacity. A well-structured 12-month Security Awareness Campaign should be mapped out. Use our Security Awareness Campaign Planner to help you develop a years' worth of awareness activities and provide structure to your employee communications.

Establish a Baseline:

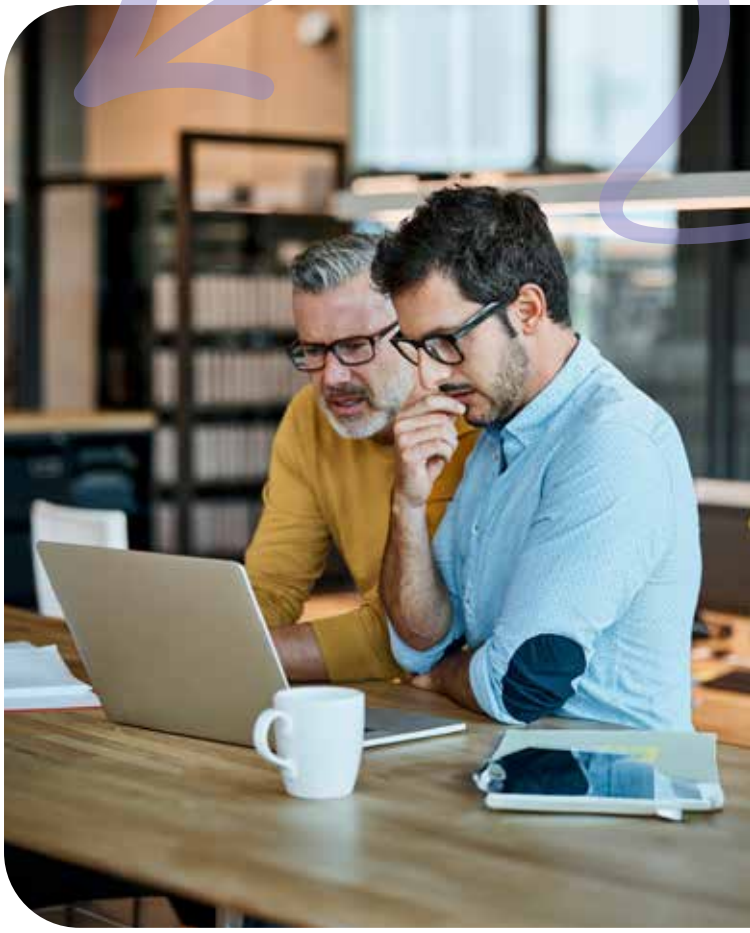
Establishing a baseline by using phishing simulations, quizzes, and surveys helps determine the starting point for your training program. These initial assessments allow for benchmarking and help set priorities by providing a clear picture of current awareness levels.

Secure Executive Support:

Securing executive support is crucial at this stage; when leaders actively participate in and promote the training program, it reinforces the importance of cyber security across the entire organisation.

Communication Strategy:

A clear communication strategy should also be developed to inform employees about the training objectives and schedule. This plan should provide details on how to access the training, the platform used, the email addresses to expect notifications from, and what users can anticipate in terms of content. With these preparations completed, the organisation is ready to move forward with implementation.



Phase 2: Implementation

Launch Awareness Campaigns:

The implementation phase begins with launching awareness campaigns to generate excitement and buy-in across the organisation. Internal communication, such as posters, emails, and meetings, plays a vital role in building momentum.

Phishing Simulations:

Once the training is underway, phishing simulations should be introduced to assess employees' awareness and identify individuals or groups at higher risk. Employees who fail phishing tests serve as an early warning sign, and those with repeated failures should receive additional attention. Implementing targeted learning experiences that reinforce the common signs of phishing emails is crucial for helping these employees recognise and avoid real phishing threats.

Regular Updates:

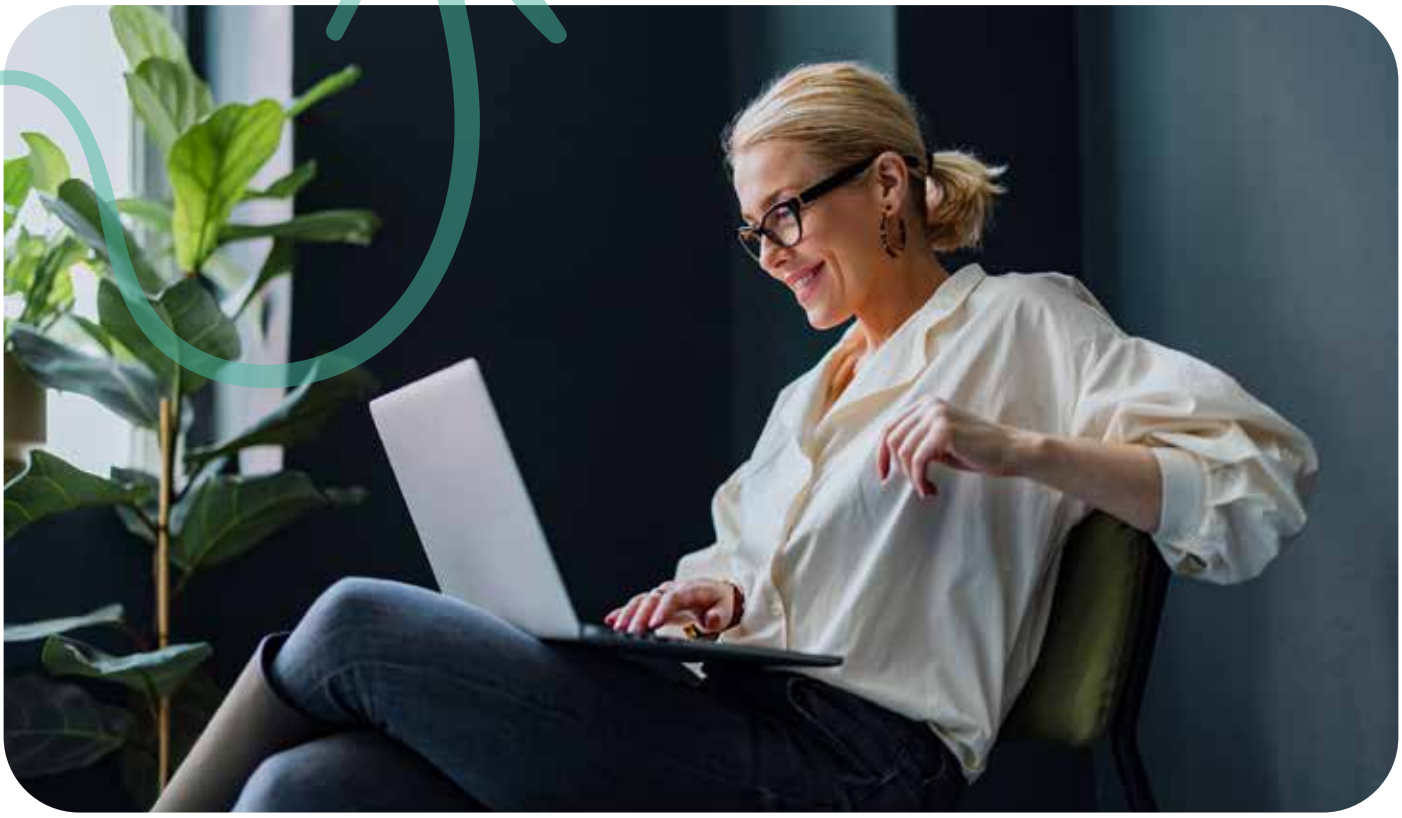
To keep employees engaged, it's important to release new content periodically. This could include newsletters, module updates, or new security scenarios that address emerging threats.

Monitor Participation:

Keeping track of who has completed the training and sending reminders to those who haven't ensures that all employees are engaged.

Assess Knowledge Retention:

Quizzes, tests, and interactive elements can be used to assess how well employees understand and retain the training content. This feedback will be vital in the next phase when reviewing and enhancing the program.



Phase 3: Review & Enhancement

Review Program Effectiveness:

The final phase of the roadmap focuses on reviewing the program's effectiveness and making ongoing improvements. Start by analysing the impact of the training through surveys, phishing simulation results, and security incident data. This analysis helps determine whether there has been a decrease in incidents, such as successful phishing attempts or data breaches. Gathering employee feedback is also important, as it can highlight strengths and identify areas where the program needs improvement.

Update Training Content:

To ensure that the training stays relevant, the content should be regularly updated to address emerging threats and changes in regulations or policies. Incorporating feedback and real-world security data allows for continuous improvement of the training material. Tailoring future training to the specific needs of departments or individuals based on their performance further enhances its effectiveness.

Benchmark Against Industry Standards:

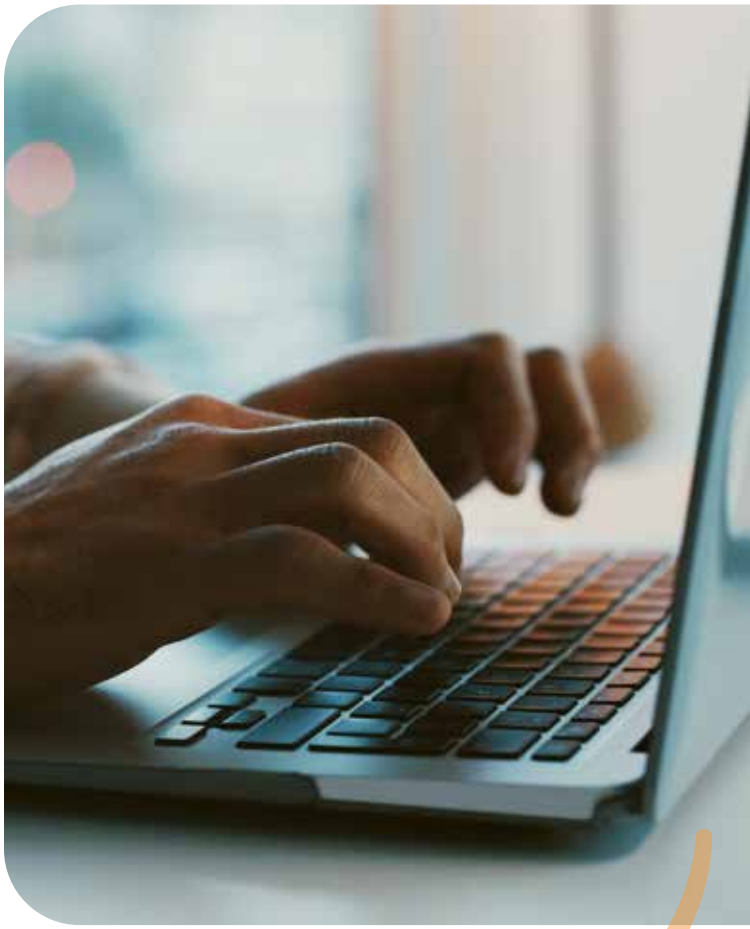
Benchmarking against industry standards provides another layer of assurance that the program is comprehensive and effective. Answer our 15-question assessment to evaluate your security awareness program and receive tailored recommendations for improvement.

Conduct Audits:

Regular audits should be conducted to assess the overall security posture and identify any gaps that the training program needs to address.

Plan for Ongoing Training:

To maintain a strong security culture, it's important to plan for ongoing training. Establishing a continuous learning strategy with periodic refreshers, updates, and advanced training ensures that employees remain vigilant and informed about evolving threats.



By following this roadmap, organisations can create a dynamic and effective Security Awareness Training program that not only educates employees but also significantly reduces security risks across the board.