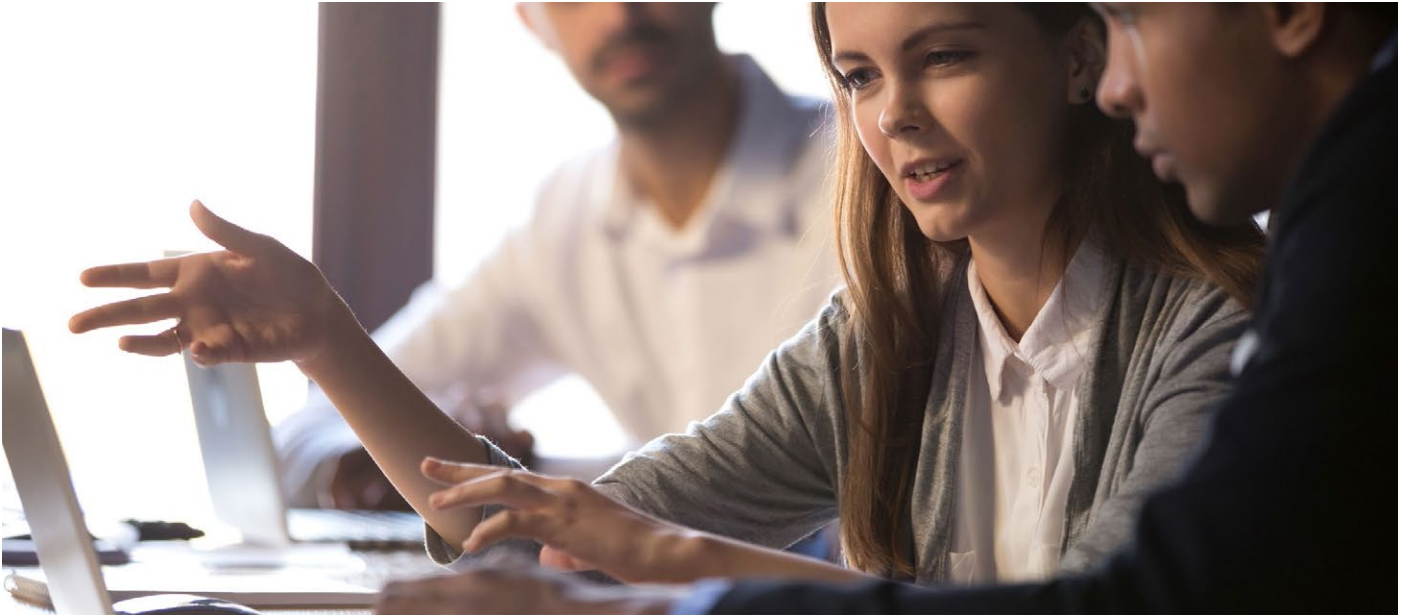


# Cybersecurity Tabletop Exercise

Strengthen response processes through realistic cyber scenarios crafted specifically for individual organizations



## Benefits

- **Increase** cyber readiness
- **Build** and strengthen teams
- **Provide** security awareness training
- **Support** regulatory compliance

Tabletop exercises provide organizations real-world scenario experience and provide peace of mind that they can be better prepared to respond to security incidents. They help ensure cybersecurity posture and workflows are in alignment with best practices

OpenText Cybersecurity Services works with organizations to create focused, organizationally relevant tabletop exercises. The team leverages decades of expertise to develop simulations and training specifically for individual organizations. Three levels of tabletop exercises are offered:

- **Level 1** - Tabletop exercises derived from potential cyber scenarios that organizations could face.
- **Level 2** - Tabletop exercises included above, plus additional content scoped from the individual organization's policies and procedures, providing a more in-depth training experience and a greater level of detail.
- **Level 3** - Red Team/Blue Team exercises – real-world role-play scenarios that identify potential gaps or improvement opportunities in the response process.

## Increase cyber readiness

Well designed and crafted tabletop exercises can improve an organization's cyber readiness. Through realistic scenarios, teams can simulate a response to cyber incidents in order to assess effectiveness. Strengths and challenges can be measured through these training events and consequently drive improvements. OpenText assists organizations to build improvements post-exercise to develop a plan of action to better identify and respond to security incidents.

## Build and strengthen teams

Team relationships are strengthened through exercises and tabletop exercises bring together the functional areas of an organization that take part in a cyber incident response. Typically, the executive team, information technology, information security, human resources, and other areas are included in the tabletop exercises. By working together, team members gain a better understanding of other areas, roles, and response measures. This better prepares overall organizational response when an incident occurs.

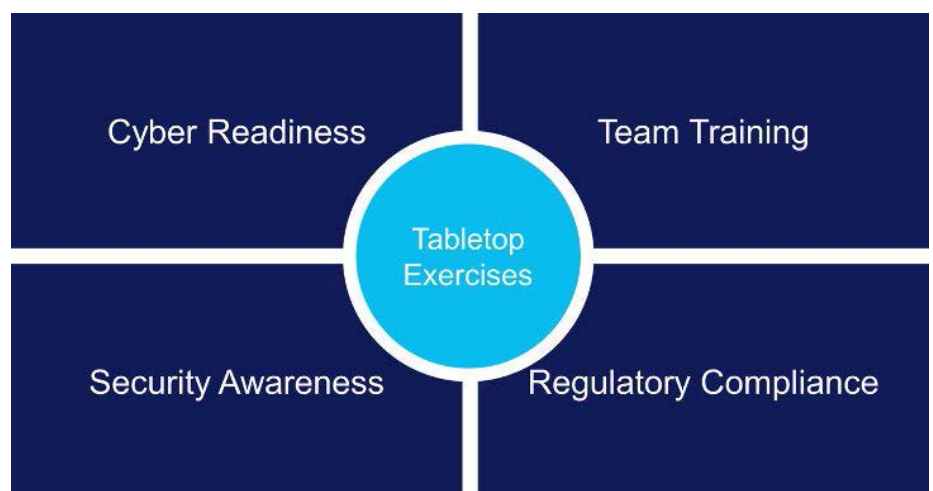
## Provide security awareness training

Many organizations have security awareness training. OpenText can tailor tabletop exercises to incorporate this training to meet the organization's requirements. The team will assess any current needs and ensure that training standards are met.

Security training is important for organizations to increase security awareness across different functions so that employees better understand when to report a security incident. It provides an explanation of risks that may be encountered in day-to-day activities and who to report them to.

## Support regulatory compliance

Many industries must meet regulatory requirements to protect information or maintain cyber compliance. These regulations can range from PCI to HIPAA to governmental regulations. The OpenText Cybersecurity Services team draws experience from a range of industries such as Defense, Engineering, Healthcare, Government, and Finance. The team has the expertise to help organizations achieve and maintain compliance no matter the industry.



Tabletop exercise benefits

## Additional Security Services

[Security Health Check ›](#)

[Threat Hunting Service ›](#)

## Tabletop exercise deliverables

**Tabletop exercise:** The exercise, comprised of one cyber scenario will be crafted specifically for the organization with specific tailored individual exercises, which contain current and relevant scenarios.

**Executive summary and report:** A post-exercise report outlining and detailing all areas of the exercise is provided.

**Policies, plans, and procedures review:** The organization's governing documentation tied to the scenario is reviewed and incorporated into the training curriculum.

## Who are OpenText Cybersecurity Services?

OpenText is an industry leader in cybersecurity solutions with more than 20 years of professional and technical expertise. Consultants hold certifications such as EnCe (OpenText Forensic (EnCase) Certified Examiner), CFSR (Certified Forensic Security Responder), EnCEP (OpenText Forensic (EnCase) Certified eDiscovery Practitioner), CISA (Certified Information System Auditor), CISSP (Certified Information Systems Security Professional), and CompTIA Security+.

For more information, please contact us at [securityservices@opentext.com](mailto:securityservices@opentext.com) or [learn more](#)

## About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: [opentext.com](https://opentext.com).