Information Security Culture

Self-assessment Survey

It's never been more important to protect the information in your organization

Cyber-attacks have become more prevalent and sophisticated, supply chains are more complex, and the volume of important information handled by organizations continues to increase. Creating a culture whereby the importance of information security is promoted and embraced avoids confusion and provides clarity.

Before you can work on ensuring an information security culture is embedded in your organization you need to understand where you are now. Take this quick quiz to determine what kind of security culture you have?

	1 = Not really				5 Absolutely
Does your leadership actively promote and communicate the importance of an information security culture?	1 ○	2 ○	3 ○	4 ○	5 ○
Are there policies and procedures in place and communicated that address critical aspects of an information security culture and the impact in the workplace?	1 ○	2 ○	3 ○	4 ○	5 ○
Have the internal and external issues that may impact your information security culture been considered?	1 ○	2 ○	3 ○	4 ○	5 ○
Does your leadership reward and recognize those people that embrace the information security culture?	1 ○	2 ○	3 ○	4 ○	5 ○
Has an information security risk assessment process been established to include risk acceptance criteria?	1 ○	2 ○	3 ○	4 ○	5 ○
Has an information security risk treatment plan been created?	1 ○	2 ○	3 ○	4 ○	5 ○

Continued >>

Have measurable information security objectives and targets been established, documented and communicated throughout the organization?	1 ●	2 ●	3 ●	4 ●	5 ●
If you have outsourced processes, are they appropriately controlled?	1 ●	2 ●	3 ●	4 ●	5 ●
Has documented evidence been kept to show that processes have been carried out as planned?	1 ●	2 ●	3 ●	4 ●	5 ●
Do top management undertake regular and periodic reviews of your information security culture?	1 ●	2 ●	3 ●	4 ●	5 ●
Does the output from the information security management review identify changes and improvements?	1 ●	2 ●	3 ●	4 ●	5 ●
Have you had incidents where your information security culture failed?	1 ●	2 ●	3 ●	4 ●	5 ●
Are your employees aware that information security is not just about your IT systems?	1 ●	2 ●	3 ●	4 ●	5 ●

Total your score to see how your organization embraces information security
Total possible: 65

55 to 65	You have a good understanding of the importance of information security within your organization.
40 to 55	You are well on your way to creating an information security culture in your organization
30 to 40	You have an understanding, but there are obvious areas for improvement in your information security culture.
0 to 30	Your level of understanding of the importance of an information security culture is putting your employees and your organization at risk.

ISO/IEC 27001, the standard for Information Security was created to help you implement a robust and systematic approach to managing information, protecting your organization’s reputation and making your business more resilient and responsive to threats. When you implement ISO/IEC 27001, it can help protect your reputation, save money, achieve compliance, and reduce risks.
Once a management system is in place, it's important that it is certified to ensure its long term effectiveness and continues to bring benefits to your organization. Why consider certification?

- **Demonstrate** to your customers, competitors, suppliers, staff and investors that you use industry-respected best practices.
- **Improves** overall performance, remove uncertainty and widen market opportunities.
- **Helps you** to reveal to stakeholders that your business is run effectively.
- **Ensures** that you are continually improving and refining your activities.
- **Improves** staff responsibility, commitment and motivation

Discover how BSI can help you create an information security culture and increase your information resilience.

Get started with ISO 27001
bsigroup.com/en-ZA

bsi.