



TIPS FOR INTEGRATING CLIMATE CHANGE INTO ISO/IEC 27001:2022

BY : NAHZATULSHIMA ZAINUDDIN | MARINAH SYAZWANI MOKHTAR
NURUL HUSNA KHASIM | ADLIL AMMAL MOHD KHARUL APENDI



ISO is adding new statements to existing and new management system standards. Organization is required to identify both external and internal factors for climate change that are important to its goals and that could impact its success in meeting the goals of its management system.

This integration reflects the growing awareness that climate change is not just an environmental issue but also a significant risk to businesses and their information assets. Extreme weather events, natural disasters, and disruptions to critical infrastructure can have profound consequences for data security and privacy.

Here are the **five (5) tips** organizations can follow when integrating climate change into ISO/IEC 27001:2022:

1

CONDUCT A CLIMATE RISK ASSESSMENT

Identify potential climate-related threats to your information assets, such as extreme weather events, power outages, and supply chain disruptions.

2

DEVELOP CLIMATE CHANGE RESPONSE PLANS

- Create specific plans to address identified climate risks.
- Consider business continuity and disaster recovery plans in the context of climate change.



3

ENHANCE SUPPLIER MANAGEMENT

- Evaluate your suppliers' climate-related risks and their sustainability practices.
- Incorporate climate-related criteria into supplier selection and performance management.

4



MEASURE AND REDUCE YOUR CARBON FOOTPRINT

- Assess your organization's carbon footprint related to IT operations.
- Implement energy-efficient practices and technologies.
- Consider using renewable energy sources.

5

FOSTER A CULTURE OF SUSTAINABILITY

- Raise awareness among employees about the impact of climate change on information security.
- Integrate climate change considerations into training and awareness programs.
- Encourage employee participation in sustainability initiatives.

