



Preparing for an ISO 27001 and 27002 Audit

A Step-by-Step Guide

A certification from the International Organization for Standardization (ISO) attests that your organization cares about quality.

Although voluntary, the three-year certification process is worth the effort for many enterprises—but the lengthy, two-stage audit and subsequent yearly check-ups can be more than a bit daunting.

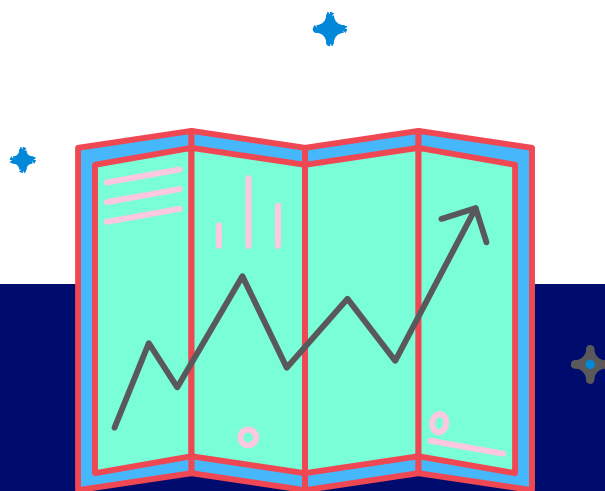
All in all, ISO has 22,000+ quality assurance standards covering manufacturing, health care, data storage, and more. While different businesses must comply with different standards, nearly all can benefit from getting certified for ISO 27001 and 27002, both of which relate to information security.

Meeting these rigorous standards assures your clients and customers that your enterprise takes security seriously. In addition, the certification process can help you comply with other frameworks, such as PCI DSS (if you collect credit card data) and HIPAA (for healthcare providers).

Checking off all the boxes you need for your ISO audit can feel overwhelming, especially at audit time. It's the culmination of three years' planning and work—where the rubber meets the road. Will you pass the test?

The answer lies not only in how well you comply with ISO standards, but also in how well you have documented your efforts.

When ISO auditors knock on your door, your best bet for getting that coveted certification is to provide the auditors with organized, well-documented evidence of your security actions, correlated with the objectives outlined in ISO 27001:2013.



To help you, we have created this checklist using the ISO 27001:2013 standards. Consider it one item at a time, and it will become your road map to ISO success.

[TAKE ME TO THE CHECKLIST](#) 

The Checklist

A.5 SECURITY POLICY

Information security policy

OBJECTIVE: *To provide management with direction and support for information security in accordance with business requirements and relevant laws and regulations.*

- What information security policies does your enterprise have? What are your information security procedures? How often are these reviewed?

A.5

A.6

A.7

A.8

A.9

A.10

A.11

A.12

A.13

A.14

A.6 ORGANIZATION OF INFORMATION SECURITY

Internal organization

OBJECTIVE: To manage information security within the organization.

- What process do you use to manage information security projects?
- Who is assigned to these projects?
- How successful have these projects been? If you are adding hardware to become ISO compliant, for instance, your auditor will want to know about it.

External parties

OBJECTIVE: To maintain the security of the organization's information and processing activities that are accessed, processed, communicated with, or managed by external parties.

- How is your information security team organized or structured? This includes the internal organization, team roles and responsibilities, segregation of duties, and contact with authorities outside the organization.
- Who are your contacts for other audits, such as SOX or HIPAA? What kind of information security structure do they have? What relationships does your internal team have with these external teams?
- Do you have relationships with any special interest groups? If so, they will need to be audited, also.

A.7 ASSET MANAGEMENT

Responsibility for assets

OBJECTIVE: *To achieve and maintain appropriate protection of organizational assets.*

- What mobile or tele-networking devices (e.g., cell phones, tablets, servers, laptops) does your organization own? You will need to provide the auditor with a complete inventory.
- Who is using these devices, and for what purposes?
- What servers and systems does your organization maintain?
- What are your policies and procedures regarding these assets as they apply to:

Provisioning: What is the process for provisioning hardware? When does provisioning occur, and how often? How is it documented?

Decommissioning: What happens to devices that reach the end of their lifespan or are returned for any reason?

Upgrades and patches: How are upgrades and patches applied, and how often?

Information classification

OBJECTIVE: *To ensure that information receives an appropriate level of protection.*

- How do you classify data within your organization (e.g., as employee, third-party, or customer/client data)? Are you labeling it? Tagging it? What labels or tags are you using?
- What assets carry that labeling/tagging information in your systems?

A.8 HUMAN RESOURCES SECURITY

Prior to employment

OBJECTIVE: *To ensure that employees, contractors, and third-party users understand their responsibilities and are suitable for their roles, and to reduce the risks of theft, fraud, and misuse of facilities.*

During employment

OBJECTIVE: *To ensure that all employees, contractors and third-party users are aware of information security threats and concerns and their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.*

- How does your enterprise screen new employees? Do you conduct background checks?
- What terms of employment do you offer to new hires? Is there a probationary period?
- Do you clearly spell out employees' duties and responsibilities? Do employees have job descriptions? Are managers' responsibilities presented to them clearly and unambiguously?
- Do you require an information security awareness program or training for all employees? What kind of training do you provide? How often are workers mandated to receive this training? Do you keep track of who receives security training and when?

Termination or change of employment

OBJECTIVE: *To ensure that employees, contractors and third-party users exit an organization or change employment in an orderly manner.*

- What are your policies and procedures regarding employment termination? How soon after the termination date do employees lose access to your organization's software and systems?

A.9 PHYSICAL AND ENVIRONMENTAL SECURITY

Secure areas

OBJECTIVE: *To prevent unauthorized physical access, damage, and interference to the organization's premises and information.*

- How does your enterprise secure its buildings, rooms, and grounds? Do workers use key cards to enter the facility? Are entries and exits monitored via video?
- Is a key card scan or other security measure required to pass from one building to another, and from one floor to another? Are elevators and stairwells secured?
- What are the policies and procedures regarding lost or stolen key cards? Is the lost card deactivated so it is no longer usable?
- What are the policies and procedures regarding cards that are damaged or in need of reprogramming? When someone requests a new or reprogrammed card, how long does it take to fulfill that request?

- How does your organization secure offices, conference rooms, the data center, and offsite storage facilities for archived documents and data? Who has access to these rooms? Who can request access to the information in these rooms, and how?

Be prepared for the auditor to walk through your buildings and campus to test your security system and protocols.

Equipment security

OBJECTIVE: *To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.*

- What is your asset maintenance and upgrade policy?
- When a new server is provisioned, what is the process for “hardening” (i.e., loading) the necessary security software and settings?
- What systems and software have been reprovisioned or decommissioned?
- What's the process to approve and sign off on server hardening?
- When a server gets removed, what is the decommissioning process? How much time passes between the initial request and the completion of decommissioning? How does your enterprise dispose of the server or asset? Is it backed up before disposal? Is the asset and its data destroyed? Who performs this service?
- When are assets repurposed? What is the process for reuse?
- When are patches and upgrades applied, and how?

A.10 COMMUNICATIONS AND OPERATIONS MANAGEMENT

Operational procedures and responsibilities

OBJECTIVE: *To ensure the correct and secure operation of information processing facilities.*

This area deals with operations security, which involves protecting your organizational systems against viruses, malware, and other maladies, and making sure that systems are running smoothly and without interruptions all the time. Managing change is a critical aspect of ensuring operational security, as well.

- What security software and services do you use to safeguard your systems against cyberattacks?
- How are system log-ins and administrator activities recorded and stored? Who has access to these records?
- If a change or security event or incident occurs, what is the notification process? Who receives an alert, and when?
- What is your change management process? Do you have a written change management plan?
- Do you have a change management board? How often does it meet? What kinds of changes does it review?
- What happens if a change request gets denied?
- After a change gets approved, how long does implementation take?
- Who is responsible for authorizing changes?

- What is your capacity management policy? When your systems approach the limits of their capacity, what happens? Who gets notified? How does your enterprise handle capacity management for email accounts, servers, and your network's bandwidth?
- Are all your clocks synchronized? This is critical for time-stamping of credit card and online transactions, in particular. If your organization challenges a transaction or faces such a challenge, you will need an accurate record of the time of occurrence.

Third-party service delivery management

OBJECTIVE: *To implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements.*

None of us lives or works in a vacuum. This is especially true in the digital age—collaborative business ecosystems are essential for success. No one entity can do it all or know it all, so we rely on third-party vendors and suppliers to fill in the gaps. But how do we know that their security meets our standards?

- What are your policies and procedures for checking the security of your third-party suppliers?
- What kind of security do you require of vendors?
- Have you seen your vendors' breach-management processes and protocols, which show how they would handle a security incident?

System planning and acceptance

OBJECTIVE: *To minimize the risk of systems failures.*

- What are your security policies for notifications regarding changes to your servers?
- Do you have an information transfer protocol that includes cryptography and key management?
- How do your servers communicate with one another? Are they still using SSL—an outdated cryptography for intra-server communication—or the more current TLS 1.2?

Protection against malicious and mobile code

OBJECTIVE: *To protect the integrity of software and information.*

- How do you ensure that newly-installed software is secure?
- How do you track requests for the software?
- How do you ensure that only approved software gets installed on your network devices?

Back-up

OBJECTIVE: *To maintain the integrity and availability of information and information processing facilities.*

- How do you back up your systems, and how often?
- Where and how do you store your backup data? Who has access to it?
- How do you secure this data?

Network security management

OBJECTIVE: *To ensure the protection of information in networks and its supporting infrastructure.*

- Do you have server redundancies, i.e., servers in colocation facilities that can be deployed if you need to restore systems from backups, conduct load balancing, or perform maintenance on all servers?
- Do you have a data center? How is it secured? How do you protect your data records and intellectual property rights?

Media handling

OBJECTIVE: *To prevent the unauthorized disclosure, modification, removal, and destruction of assets, and to avoid the associated interruption to business activities.*

This section refers to the security and transfer of media contained on flash drives or computer discs. Some organizations allow the reuse of these drives and discs, while others require disposal after one use.

- What are your policies regarding the viewing, sharing, and downloading of media onto enterprise devices from flash drives or discs?
- What happens to the drives or discs once they have served their initial purpose? Do you require disposal? How do you enforce it? Who disposes of the drives or discs, and do they wipe the devices clean of media beforehand?
- Under what circumstances do you allow reuse of discs and flash drives? What are the protocols and procedures for removing the information they contain? What happens to that data? Who can access it?

Exchange of information

OBJECTIVE: *To maintain the security of information and software exchanged within the organization and with any external entities.*

- What are your policies and procedures regarding transfer of data and software to others within your enterprise? To those outside of it?
- Which cloud services do you authorize for software development? How do you ensure that they are secure?
- Do you allow the downloading of external applications and software onto enterprise-issued devices? If so, what firewalls are in place to protect your organization's data, networks, and systems?

Electronic commerce services

OBJECTIVE: *To ensure the security of electronic commerce services and their secure use.*

- Does your business accept credit cards or online purchases?
- Do you store any customer data, including financial data? Where is it stored, and for how long?
- Is stored financial data "anonymized" (identifying information has been removed) or "pseudonymized" (identifying information has been replaced so that it is unidentifiable)?
- Who has access to this data?

Monitoring

OBJECTIVE: To detect unauthorized information processing activities.

- How do you monitor your networks and systems to detect unauthorized activity?
- If suspicious activity is detected, who gets notified, and how quickly? What are the follow-up procedures?

A.11 ACCESS CONTROL

Business requirement for access control

OBJECTIVE: To control access to information.

- Who has access to your systems, network, and applications?
- How do users gain access? How are they removed from your system?
- If you implement new systems or assets and hire or contract with people to build software or install hardware, what activation and deactivation controls do you have in place?
- How do you track the activities of contracted workers in your systems and network? Do you provide full access, or restrict workers to the areas necessary for their job? When they finish the job, how do you remove their access, and within what timeframe?

User access management

OBJECTIVE: *To ensure authorized user access and to prevent unauthorized access to information systems.*

- How do you determine who gets access to which areas of your systems and network?
- How do you authenticate users? Do you use multi-factor authentication?
- How do you set up authentication? Do you use a device, biometrics, or push notifications with codes?

User responsibilities

OBJECTIVE: *To prevent unauthorized user access, and compromise or theft of information and information processing facilities.*

Network access control

OBJECTIVE: *To prevent unauthorized access to networked services.*

Operating system access control

OBJECTIVE: *To prevent unauthorized access to operating systems.*

- Who has access to your systems? Who has access to your network and applications?

- How are users granted access? How are they removed from the system?
- How do you track the activities of external vendors in your systems? How do you limit their access? When they finish their contract, how long does it take to remove their access?

Application and information access control

OBJECTIVE: To prevent unauthorized access to information held in application systems.

- How do you manage developers' access to application systems information?
- Do you require one set of credentials for developers, and another for the team members who push the application data into production? These should not be the same people.

Mobile computing and teleworking

OBJECTIVE: To ensure information security when using mobile computing and teleworking facilities.

- What are your password management policies?
- Do you require a password for every use of your organizational devices?
- Do you require the use of complex passwords with at least 12 characters comprising a mix of letters, numbers, and symbols?
- Have you programmed passwords to expire and require periodic replacement? How often do you require this?

A.12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE

Security requirements of information systems

OBJECTIVE: To ensure that security is an integral part of information systems.

- Do sensitive utility programs have restricted, “privileged user” access? Who has this access, and how do they use it?
- How do you monitor changes to these high-level programs?
- When developers make changes to programs, are they doing so strictly in the development environment?
- Does a second party or team move changes into production?
- Does your development process incorporate privacy by design?

Cryptographic controls

OBJECTIVE: To protect the confidentiality, authenticity, and integrity of information by cryptographic means.

- How do you transmit your data? Do you use cryptography? What kind, and how is it applied?
- What are your key management policies?

Security of system files

OBJECTIVE: To ensure the security of system files.

- Are your assets secured against unauthorized access? This includes equipment, such as copy machines, that store information but do not transmit data. Do you erase the memory of these machines before you decommission, remove, or replace them? What process do you use?
- Have you secured your Voice over Internet Protocol (VoIP), voice mail, and landline telephone systems? Do your processes for removal or replacement include erasing the system's memory?
- What are your policies and procedures for securing supporting utilities associated with your data systems? Cables, routers, and any other peripheral devices related to your network can be hacked, too.

Security in development and support processes

OBJECTIVE: To maintain the security of application system software and information.

Auditors, especially those with experience in IT, tend to be sticklers about the separation of development, testing, and production environments.

- When your development teams finish programming, do they stop and push their work into the staging or testing environment?

- Does a second team test the developers' work independently? Verification and testing are critical for spotting and correcting vulnerabilities that could allow hackers to gain entry into your systems.
- Does a third person or team move the tested software into production? The person who wrote the code or piece of software should never move it into production.

Technical vulnerability management

OBJECTIVE: To reduce the risks associated with the exploitation of published technical vulnerabilities.

Vulnerability management, patch management, and timely upgrades are critical for IT security. Failure to patch software promptly is a leading cause of data breaches and will raise red flags for auditors.

- Do you conduct penetration testing on new systems and those that run confidential data? How have you resolved any identified issues?
- Do you regularly scan your systems, networks, and software for vulnerabilities? How often do you conduct these scans? What happens when you find issues?
- Have you documented your vulnerability plan, remediation plan, project plan, and project plan status? Your auditor will want to see them.
- How do you restrict software installation on company-owned devices?
- Unauthorized software may contain viruses.

A.13 INFORMATION SECURITY INCIDENT MANAGEMENT

Reporting information security events and weaknesses

OBJECTIVE: *To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.*

Management of information security incidents and improvements

OBJECTIVE: *To ensure a consistent and effective approach is applied to the management of information security incidents.*

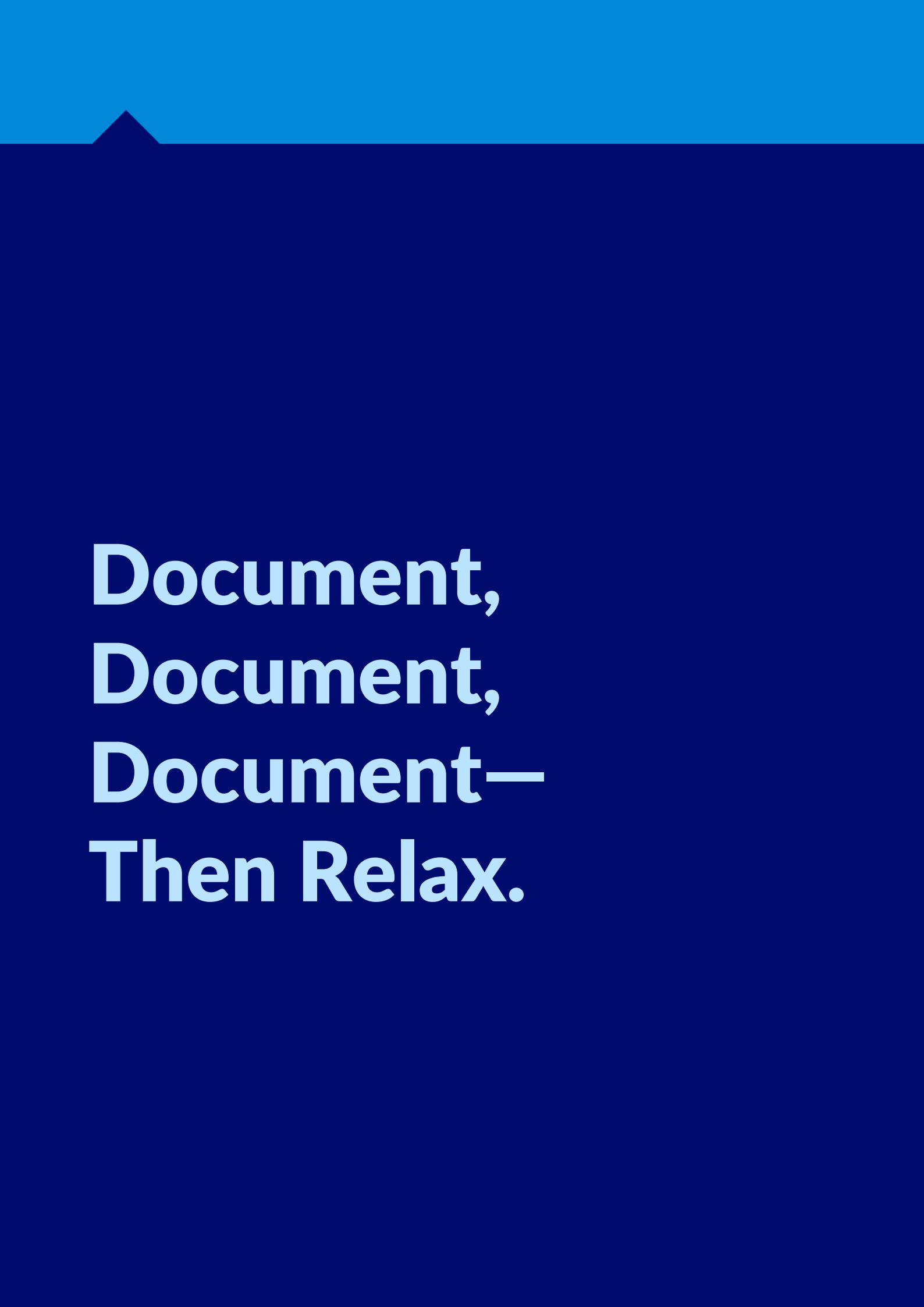
- What are your policies and procedures for responding to system and network vulnerabilities, breach attempts, and breaches? Do employees know their roles? Who gets notified, and what is the chain of command?
- Do you have an incident response plan, and are the appropriate people familiar with it?

A.14 BUSINESS CONTINUITY MANAGEMENT

Information security aspects of business continuity management

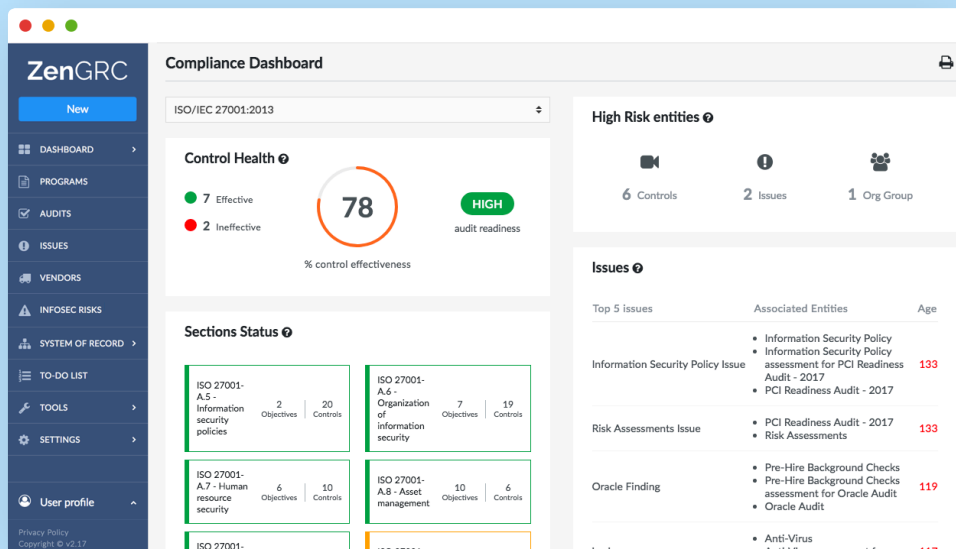
OBJECTIVE: *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.*

- Do you know the risks posed to your organization by natural disasters?
- How is your organization protected against external environmental threats such as fires and earthquakes?
- What is the process and protocol to protect the business in the event of a disaster? How will you protect the organization's data?
- Should disaster strike, how quickly must the business recover?
- Be prepared to provide your Disaster Recovery and Business Continuity Plans.



**Document,
Document,
Document—
Then Relax.**

As always when dealing with auditors, it is a good idea not only to prepare answers to their anticipated questions, but also to support your answers with documentation. As you work through this checklist, consider which documents you need for this purpose, and be ready to provide them for the auditor's perusal.



But the single best way to get ready for the extensive and thorough ISO audit is to conduct an internal audit in advance. Your internal auditors may use this checklist to help pinpoint any deficiencies or trouble spots, or you may wish to use a quality risk and compliance software with self-auditing capabilities.

ISO 27001 and 27002 require rigorous and lengthy processes, but that should not dissuade you from pursuing this prize. If it were easy, everyone would do it, right?

.....

Going the extra distance to obtain the ISO certification will set your enterprise apart from the rest, attesting that you care not only about quality, but also about security—which, in this day and age, are often the same thing.

.....

The Checklist

A.5 SECURITY POLICY

Information security policy

- What information security policies does your enterprise have? What are your information security procedures? How often are these reviewed?

A.6 ORGANIZATION OF INFORMATION SECURITY

Internal organization

- What process do you use to manage information security projects?
- Who is assigned to these projects?
- How successful have these projects been? If you are adding hardware to become ISO compliant, for instance, your auditor will want to know about it.

External parties

- How is your information security team organized or structured? This includes the internal organization, team roles and responsibilities, segregation of duties, and contact with authorities outside the organization.
- Who are your contacts for other audits, such as SOX or HIPAA? What kind of information security structure do they have? What relationships does your internal team have with these external teams?
- Do you have relationships with any special interest groups? If so, they will need to be audited, also.

A.7 ASSET MANAGEMENT

Responsibility for assets

- What mobile or tele-networking devices (e.g., cell phones, tablets, servers, laptops) does your organization own? You will need to provide the auditor with a complete inventory.
- Who is using these devices, and for what purposes?
- What servers and systems does your organization maintain?
- What are your policies and procedures regarding these assets as they apply to:
 - Provisioning: What is the process for provisioning hardware? When does provisioning occur, and how often? How is it documented?
 - Decommissioning: What happens to devices that reach the end of their lifespan or are returned for any reason?
 - Upgrades and patches: How are upgrades and patches applied, and how often?

Information classification

- How do you classify data within your organization (e.g., as employee, third-party, or customer/client data)? Are you labeling it? Tagging it? What labels or tags are you using?
- What assets carry that labeling/tagging information in your systems?

A.8 HUMAN RESOURCES SECURITY

During employment

- How does your enterprise screen new employees? Do you conduct background checks?
- What terms of employment do you offer to new hires? Is there a probationary period?
- Do you clearly spell out employees' duties and responsibilities? Do employees have job descriptions? Are managers' responsibilities presented to them clearly and unambiguously?
- Do you require an information security awareness program or training for all employees? What kind of training do you provide? How often are workers mandated to receive this training? Do you keep track of who receives security training and when?

Termination or change of employment

- What are your policies and procedures regarding employment termination? How soon after the termination date do employees lose access to your organization's software and systems?

A.9 PHYSICAL AND ENVIRONMENTAL SECURITY

Secure areas

- How does your enterprise secure its buildings, rooms, and grounds? Do workers use key cards to enter the facility? Are entries and exits monitored via video?
- Is a key card scan or other security measure required to pass from one building to another, and from one floor to another? Are elevators and stairwells secured?
- What are the policies and procedures regarding lost or stolen key cards? Is the lost card deactivated so it is no longer usable?
- What are the policies and procedures regarding cards that are damaged or in need of reprogramming? When someone requests a new or reprogrammed card, how long does it take to fulfill that request?
- How does your organization secure offices, conference rooms, the data center, and offsite storage facilities for archived documents and data? Who has access to these rooms? Who can request access to the information in these rooms, and how?

Equipment security

- What is your asset maintenance and upgrade policy?
- When a new server is provisioned, what is the process for "hardening" (i.e., loading) the necessary security software and settings?
- What systems and software have been reprovisioned or decommissioned?
- What's the process to approve and sign off on server hardening?
- When a server gets removed, what is the decommissioning process? How much time passes between the initial request and the completion of decommissioning? How does your enterprise dispose of the server or asset? Is it backed up before disposal? Is the asset and its data destroyed? Who performs this service?

- When are assets repurposed? What is the process for reuse?
- When are patches and upgrades applied, and how?

A.10 COMMUNICATIONS AND OPERATIONS MANAGEMENT

Operational procedures and responsibilities

- What security software and services do you use to safeguard your systems against cyberattacks?
- How are system log-ins and administrator activities recorded and stored? Who has access to these records?
- If a change or security event or incident occurs, what is the notification process? Who receives an alert, and when?
- What is your change management process? Do you have a written change management plan?
- Do you have a change management board? How often does it meet? What kinds of changes does it review?
- What happens if a change request gets denied?
- After a change gets approved, how long does implementation take?
- Who is responsible for authorizing changes?
- What is your capacity management policy? When your systems approach the limits of their capacity, what happens? Who gets notified? How does your enterprise handle capacity management for email accounts, servers, and your network's bandwidth?
- Are all your clocks synchronized? This is critical for time-stamping of credit card and online transactions, in particular. If your organization challenges a transaction or faces such a challenge, you will need an accurate record of the time of occurrence.

Third-party service delivery management

- What are your policies and procedures for checking the security of your third-party suppliers?
- What kind of security do you require of vendors?
- Have you seen your vendors' breach-management processes and protocols, which show how they would handle a security incident?

System planning and acceptance

- What are your security policies for notifications regarding changes to your servers?
- Do you have an information transfer protocol that includes cryptography and key management?
- How do your servers communicate with one another? Are they still using SSL—an outdated cryptography for intra-server communication—or the more current TLS 1.2?

Protection against malicious and mobile code

- How do you ensure that newly-installed software is secure?
- How do you track requests for the software?
- How do you ensure that only approved software gets installed on your network devices?

Back-up

- How do you back up your systems, and how often?
- Where and how do you store your backup data? Who has access to it?
- How do you secure this data?

Network security management

- Do you have server redundancies, i.e., servers in colocation facilities that can be deployed if you need to restore systems from backups, conduct load balancing, or perform maintenance on all servers?
- Do you have a data center? How is it secured? How do you protect your data records and intellectual property rights?

Media handling

- This section refers to the security and transfer of media contained on flash drives or computer discs. Some organizations allow the reuse of these drives and discs, while others require disposal after one use.
- What are your policies regarding the viewing, sharing, and downloading of media onto enterprise devices from flash drives or discs?
- What happens to the drives or discs once they have served their initial purpose? Do you require disposal? How do you enforce it? Who disposes of the drives or discs, and do they wipe the devices clean of media beforehand?
- Under what circumstances do you allow reuse of discs and flash drives? What are the protocols and procedures for removing the information they contain? What happens to that data? Who can access it?

Exchange of information

- What are your policies and procedures regarding transfer of data and software to others within your enterprise? To those outside of it?
- Which cloud services do you authorize for software development? How do you ensure that they are secure?
- Do you allow the downloading of external applications and software onto enterprise-issued devices? If so, what firewalls are in place to protect your organization's data, networks, and systems?

Electronic commerce services

- Does your business accept credit cards or online purchases?
- Do you store any customer data, including financial data? Where is it stored, and for how long?
- Is stored financial data "anonymized" (identifying information has been removed) or "pseudonymized" (identifying information has been replaced so that it is unidentifiable)?
- Who has access to this data?

Monitoring

- How do you monitor your networks and systems to detect unauthorized activity?
- If suspicious activity is detected, who gets notified, and how quickly? What are the follow-up procedures?

A.11 ACCESS CONTROL

Business requirement for access control

- Who has access to your systems, network, and applications?
- How do users gain access? How are they removed from your system?
- If you implement new systems or assets and hire or contract with people to build software or install hardware, what activation and deactivation controls do you have in place?

- How do you track the activities of contracted workers in your systems and network? Do you provide full access, or restrict workers to the areas necessary for their job? When they finish the job, how do you remove their access, and within what timeframe?

User access management

- How do you determine who gets access to which areas of your systems and network?
- How do you authenticate users? Do you use multi-factor authentication?
- How do you set up authentication? Do you use a device, biometrics, or push notifications with codes?

Operating system access control

- Who has access to your systems? Who has access to your network and applications?
- How are users granted access? How are they removed from the system?
- How do you track the activities of external vendors in your systems? How do you limit their access? When they finish their contract, how long does it take to remove their access?

Application and information access control

- How do you manage developers' access to application systems information?
- Do you require one set of credentials for developers, and another for the team members who push the application data into production? These should not be the same people.

Mobile computing and teleworking

- What are your password management policies?
- Do you require a password for every use of your organizational devices?
- Do you require the use of complex passwords with at least 12 characters comprising a mix of letters, numbers, and symbols?
- Have you programmed passwords to expire and require periodic replacement? How often do you require this?

A.12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE

Security requirements of information systems

- Do sensitive utility programs have restricted, "privileged user" access? Who has this access, and how do they use it?
- How do you monitor changes to these high-level programs?
- When developers make changes to programs, are they doing so strictly in the development environment?
- Does a second party or team move changes into production?
- Does your development process incorporate privacy by design?

Cryptographic controls

- How do you transmit your data? Do you use cryptography? What kind, and how is it applied?
- What are your key management policies?

Security of system files

- Are your assets secured against unauthorized access? This includes equipment, such as copy machines, that store information but do not transmit data. Do you erase the memory of these machines before you decommission, remove, or replace them? What process do you use?
- Have you secured your Voice over Internet Protocol (VoIP), voice mail, and landline telephone systems? Do your processes for removal or replacement include erasing the system's memory?
- What are your policies and procedures for securing supporting utilities associated with your data systems? Cables, routers, and any other peripheral devices related to your network can be hacked, too.

Security in development and support processes

- When your development teams finish programming, do they stop and push their work into the staging or testing environment?
- Does a second team test the developers' work independently? Verification and testing are critical for spotting and correcting vulnerabilities that could allow hackers to gain entry into your systems.
- Does a third person or team move the tested software into production? The person who wrote the code or piece of software should never move it into production.

Technical vulnerability management

- Do you conduct penetration testing on new systems and those that run confidential data? How have you resolved any identified issues?
- Do you regularly scan your systems, networks, and software for vulnerabilities? How often do you conduct these scans? What happens when you find issues?
- Have you documented your vulnerability plan, remediation plan, project plan, and project plan status? Your auditor will want to see them.
- How do you restrict software installation on company-owned devices? Unauthorized software may contain viruses.

A.13 INFORMATION SECURITY INCIDENT MANAGEMENT

Management of information security incidents and improvements

- What are your policies and procedures for responding to system and network vulnerabilities, breach attempts, and breaches? Do employees know their roles? Who gets notified, and what is the chain of command?
- Do you have an incident response plan, and are the appropriate people familiar with it?

A.14 BUSINESS CONTINUITY MANAGEMENT

Information security aspects of business continuity management

- Do you know the risks posed to your organization by natural disasters?
- How is your organization protected against external environmental threats such as fires and earthquakes?
- What is the process and protocol to protect the business in the event of a disaster? How will you protect the organization's data?
- Should disaster strike, how quickly must the business recover?
- Be prepared to provide your Disaster Recovery and Business Continuity Plans.

About ZenGRC

ZenGRC provides the world's leading companies.

Our cloud-based solution with fast, easy deployment, unified controls management, and a centralized dashboard offers simple, streamlined compliance and risk management, including self-audits, without the hassle and confusion of spreadsheets. Contact a ZenGRC expert today to request your free demo, and embark on the worry-free path to regulatory compliance—the Zen way.

www.ZenGRC.com/resources

engage@ZenGRC.com

(877) 440-7971