TEVORA™ | White Paper

Guide to Implementing ISO 22301 Standards for Organizational Resilience and Compliance

Jonathan Lee
June 14, 2022

Table of Contents

Introduction

Effective business continuity has become essential to any successful organization in a world rife with ransomware, global pandemics, and provider shortages. With its focus on preparing in advance for potential disruptions, business continuity planning helps organizations ensure they can still perform critical business functions when problems occur.

An organization's customers, stakeholders, and business partners consistently depend on it to deliver products and services. To meet these expectations, it's not enough to rely on spur-of-the-moment reactions or snap judgments to respond to disruptions. Organizations must plan for inevitable disruptions by developing a Business Continuity Management System (BCMS), which includes the resources, plans, and policies necessary to ensure organizational resiliency.

What is a BCMS?

A BCMS is the industry-standard approach to delivering strong business continuity. As organizations increasingly choose to invest in building up their business continuity capabilities, the International Organization for Standardization (ISO) has developed the ISO 22301 standard to help guide organizations through this process. This standard is the industry gold standard for business continuity planning. It details the critical facets of an effective BCMS and how to keep the management system robust and effective over time. Organizations can use the standard to inform goals and decisions for improving business continuity. Once established an effective BCMS, an organization can pursue full ISO 22301 certification to demonstrate its ability to remain operational during a disruption.

Why Get ISO 22301 Certified?

Organizations can apply ISO 22301 simply as a model for their own BCMS or pursue full ISO 22301 certification, which requires being audited by an official ISO 22301 certifying body. Certified organizations demonstrate to customers and business partners that they will be resilient during disruptions and can be trusted to provide their products or services as expected. Certification also gives organizations a competitive advantage as some ISO 22301-certified organizations only partner with other certified organizations. Other benefits include legal compliance, customer satisfaction, and resiliency during unexpected circumstances such as server outages, cyberattacks, and pandemics. This competitive advantage leads more organizations to invest in business continuity improvements and ISO 22301 certification.

This white paper aims to offer practical guidance to organizations wishing to become ISO 22301 compliant.

ISO 22301 at a Glance

ISO 22301 is a framework that helps organizations build an effective BCMS. It is divided into eleven clauses, from 0 to 10, each describing the purpose of the standard or specific requirements to fulfill. The first section, Clause 0, details a management system and how the rest of the document is laid out. Critically, it touches on the components of a management system, including a policy, competent people with defined responsibilities, documented information supporting the controls, and management processes related to policy, planning, implementation, performance assessment, management review, and continual improvement.

Clauses 1-3

Clauses 1, 2, and 3 mostly describe supplementary details and are nearly identical to the corresponding first three clauses in other ISO standards. Clause 1 explains the scope of ISO 22301, which is intended for organizations of any size, nature, and type. Clause 2 clarifies that this standard borrows terms and definitions from other documents, specifically ISO 22300, which defines common security and resiliency terms. Clause 3 lists additional terms and definitions specific to this document.

Clauses 4, 5, 6, and 7 detail the setup phase of implementing a BCMS. Like other management systems from ISO, a BCMS under ISO 22301 requires four supporting components to ensure the business continuity plans and strategies are carried out effectively. These components are leadership, planning, and support, each of which is represented by a separate clause.

Clause 4

WHAT: Clause 4 focuses on the organization's context and how that determines the scope of its BCMS. This context includes external relationships with other interested parties (e.g., stakeholders, clients, or business partners) and internal obligations. In terms of external factors, an organization should consider the legal, market, and cultural environment it operates in and any expectations from that environment, such as regulations or laws it must comply with. The organization should also identify outside organizations that rely on its products or services. Likewise, an organization should consider internal factors such as its mission, nature, and goals. Taken together, this information should be used to establish a defined scope that identifies the parts of the organization the BCMS encompasses. Any details or units not covered by the BCMS must have a documented reason for their exclusion, which explains why they are not critical to the organization's business continuity capacities.

HOW: An organization adequately considers its context by documenting this scope alongside the legal, regulatory, and other requirements described above. This documentation must be kept updated with current information, especially the abovementioned requirements.

Clause 5

WHAT: Clause 5 focuses on the roles and responsibilities of the organization's leadership concerning its BCMS. Leadership, or top management, as ISO 22301 describes it, is responsible for integrating the BCMS into the organization and paying for the resources necessary to support it. This includes promoting conformity to the BCMS, communicating its importance across the organization, and supporting continual improvement. Leadership must also create a documented business continuity policy, which defines a framework for determining business continuity objectives to be met during a disruption. Finally, leadership should delegate roles and responsibilities for the operation of the BCMS, including reviewing the BCMS and reporting results back to leadership.

HOW: Leadership can meet these requirements by creating a Governance Document, which includes the organization's business continuity and disaster recovery policies. By developing a Governance Document, communicating it to the organization, and supporting its application, leadership can fulfill its business continuity responsibilities under Clause 5.

Clause 6

WHAT: Clause 6 covers the planning of goals for the BCMS. An organization starts by determining the potential risks that could hinder or obstruct its BCMS, then develops plans to address the identified risks. It also documents a set of business continuity objectives: the goals the organization intends to meet regarding its ability to continue operating in a disruption. The clause also notes that changes to the BCMS should be planned with an eye toward feasibility and potential consequences.

HOW: An organization can meet this requirement by taking the time to carefully decide on business continuity objectives. These objectives should be documented either in a Governance Document or in separate documents referenced by the Governance Document. The organization should also conduct deliberate and thorough planning when addressing potential risks and making changes to the BCMS.

Clause 7

WHAT: Clause 7 focuses on providing the resources necessary for operation of the BCMS. It emphasizes the importance of having competent personnel with adequate training to do their work effectively and awareness of their roles and responsibilities in support of the BCMS. The clause describes an organization's need to define how and when it will communicate internally and externally regarding the BCMS. Finally, the organization must document all information related to the BCMS. The documentation should be kept up to date and available to the appropriate parties.

HOW: An organization can meet these requirements by recording all this information in documents contained in the BCMS. Common industry practice is defining and organizing governing policies for each requirement in the Governance Document. The Governance Document then references separate documents, which describe in more detail the modes of communication during disruption and the personnel's roles, responsibilities, and competencies.

Clause 8

WHAT: Clause 8 transitions from the setup phase of the earlier clauses to the actual operation of the BCMS. It specifies what organizations should do to address and improve business continuity. The clause consists of five main actions to perform, directed by the objectives and policies defined earlier in the setup phase.

First, organizations should conduct a Business Impact Analysis (BIA) to decide which business functions are most important and how a disruption to each function could impact the overall organization. This helps organizations establish priorities and set recovery statistics like MTPDs (Maximum Tolerable Period of Disruption) and RTOs (Recovery Time Objectives).

Next, the clause describes the requirement for a risk assessment to identify the potential and most likely disruption risks and evaluate which ones to address.

Using the results of the BIA and risk assessment, an organization moves on to developing a Business Continuity Strategy. This process involves brainstorming options for addressing the identified risks and selecting the best option for each risk.

The organization builds Business Continuity Plans based on the options for addressing risks. These are the essential documents employees will turn to and apply in the event of a disruption. The plans specify roles and responsibilities for all personnel, steps to take during a disruption, how to communicate between teams and with external parties, and the process for escalating the situation to top management or others.

Finally, ISO 22301 specifies that an organization must regularly test its Business Continuity Strategy and Business Continuity Plans, making improvements as necessary.

HOW: An organization can meet the requirements of Clause 8 by conducting each of the steps listed above. After completing a BIA and risk assessment, the organization should carefully develop a Business Continuity Strategy and Business Continuity Plans. It should define a regular testing schedule that tests those plans in real-life situations (e.g., using tabletop exercises). Then it must stick to the defined schedule and implement the necessary changes to continually improve its BCMS.

Clause 9

WHAT: Clause 9 begins a new section focused on evaluating BCMS's effectiveness. This evaluation consists of an Internal Audit and managerial review of the audit findings and other BCMS performance information. This evaluation should produce documents capturing any decisions to alter or improve the BCMS, which the organization should implement.

HOW: An organization can meet these requirements by conducting or outsourcing an Internal Audit. Once the audit has been completed, management should review the entire BCMS in light of the audit findings and decide what changes to make to improve its effectiveness. This process, along with any other monitoring systems deemed necessary, should be recorded in documentation such as a Business Continuity Documentation Review log.

Clause 10

WHAT: Clause 10 introduces the final phase, continual improvement. ISO 22301 expects organizations to perform corrective actions to address their non-conformity to the standard. Previous stages , such as management review, help the organization identify these non-conformities. As before, both issues and corrective actions should be documented.

HOW: An organization can meet this requirement by acting on the non-conformities discovered in its Internal Audit, tabletop exercises, or other evaluation activities. This includes documenting corrective actions in a record such as a Business Continuity Documentation Review log.

ISO 22301 Required Documents

As stated in Clause 1, ISO 22301 is intended to cover organizations of any type, size, and nature. Consequently, the standard itself does not list specific documents to include in a BCMS. Instead, it refers more generally to having documentation for the various requirements of a BCMS. To help organizations apply these principles in their environment, Tevora has compiled a list of documents that organizations commonly use to implement 22301. The list is divided into two sections: the first comprising policies and the second representing proof that those policies are being practiced.

Policy Documents

The following table lists policies that must be documented according to ISO 22301 and the corresponding document in which they are often implemented. Policy requirements are fulfilled by identifying a document that addresses each requirement and how the designated document is governed. This is distinct from the actual scenarios and responses, which are covered in a business continuity plan but not in a business continuity policy.

In practice, an organization fulfills a policy requirement by demonstrating that it has the required policy in place. The focus is not on the specific details or quality of the plans implementing that policy but simply that a policy exists to guide them. For example, Clause 7.2 requires an organization to "retain appropriate documented information as evidence of competence [of its personnel]." An organization can fulfill this clause by specifying in its Governance Document that it keeps track of employees' degrees, certifications, and completed training in an internal employee records database. While the records themselves are not listed in the Governance Document, the organization's goal and method for meeting that requirement is, which fulfills the policy requirement.

Clause	Requirement	Content	Often implented in
4.2.1	Legal, regulatory, and other requirements	Lists everything an organization needs to comply with	Governance document *
4.3	The scope of the BCMS and explanation of exclusions	Dedines which parts of the organization are included and excluded from the BCMS	Governance document
5.2	Business continuity policy	Defines main responsibilities, and the intent of management	Business continuity policy
7.2	Competencies of personnel	Defines knowlege and skills needed by staff with business continuity responsibilities	Governance document*
8.4.3.1	Documented procedure for communication with interested parties	These could be emailes but also social comminication from sources such as government agencies and others	Governance document*

*These requirements are typically consolidated in a governance document. However, they may also be specified in a separate document that is referenced in the governance document.

Implementation Documents

The following table lists plans, records, and results that must be documented to prove an organization has put the principles of ISO 22301 into practice. Because these entries refer to records and plans, they are fulfilled by documents and logs kept by the organization and accessible to relevant personnel. For example, Clause 9.1.1 requires an organization to "retain appropriate documented information as evidence of the results [of monitoring and measuring the BCMS]." An organization can fulfill this clause by preserving performance evaluation data and recording the date and time a manager analyzes that data for evaluation of the BCMS. In this case, the actual records of the evaluation and associated data fulfill this requirement.

Clause	Requirement	Content	Often implented in
6.2	Business continuity objectives	Defines measurable goals related to business continuity, specific to the organization's context and needs	Business continuity plans
8.2	Business impact analysis and risk assessment	The BIA Report and Risk Assessment Report	BIA Report and Risk Assessment Report
8.4.4	Business continuity policy	Detailed plans and procedures for meeting business continuity objectives in a disruption	Business continuity policy
8.5	Program of exercising and testing business continuity strategies	Define a regular pattern of scenario-based exercises to test business plans (e.g., Tabletop Exercises)	Records of Testing
9.1.1	Data and results of monitoring and measurement	Evaluation of whether BCMS meets the business continuity objectives	Records of Business Continuity Documentation Review
9.2	Internal audit program and results	The Internal Audit Report	Internal Audit Report
10.1	Nature of non-conformities and actions taken	Description of each discovered non-conformity and its cause	Records of Business Continuity Documentation Review
10.1	Results of corrective actions	Description of what actions were taken to eliminate a non-conformity	Records of Business Continuity Documentation Review

Governance Document

Primary Function	Describes the scope of the BCMS and how policies and plans will be governed, updated, implemented and removed. Lists business continuity requirements and where they are met, referencing additional supporting documents.
Clause of Origin	**CLAUSE 4.3** The organization shall: **a)** establish the parts of the organization to be included in the BCMS, taking into account its location(s), size, nature, and complexity; **b)** identify products and services to be included in the BCMS. When defining the scope, the organization shall document and explain exclusions. They shall not affect the organization's ability and responsibility to provide business continuity, as determined by the business impact analysis or risk assessment and applicable legal or regulatory requirements.
Related Clauses	4.2 5.2 6.3 7.2, 7.4, 7.5 8.4.3

DESCRIPTION

A governance document is the most comprehensive document in a BCMS and is typically among the first to be implemented. It encompasses the entire management system and defines how the other documents will be managed and organized.

A critical objective of the governance document is to establish the scope of the BCMS. This involves defining which functional units to include in the management system and which to exclude. These boundaries should be drawn based on the list of relevant legal and regulatory standards the organization must comply with. The governance document should either include this list or a reference to it.

Other policy requirements can be fulfilled in a similar fashion. A governance document can specify that it meets a given requirement by having a corresponding policy, then define that policy directly in the governance document or provide a reference to another document that contains the policy definition.

To implement a governance document, the organization should take time to analyze its context so that it can determine the appropriate boundaries for its BCMS. After documenting those boundaries as the BCMS scope, the organization should evaluate which policies to implement based on the defined scope. The governance document should specify that the organization implements each required policy and then reference where it does so, whether that is in the governance document itself, or externally in another document.

Business Impact Analysis and Risk Assessment

Primary Function	Identifies and prioritizes resources with the most impact on critical business operations so that an organization can take steps to plan for and address them.
Clause of Origin	**CLAUSE 8.2** The organization shall: **a)** implement and maintain systematic processes for analyzing the business impact and assessing the risks of disruption; **b)** review the business impact analysis and risk assessment at planned intervals and when there are significant changes within the organization or the context in which it operates.
Related Clauses	6.2 7.3 8.3, 8.4, 8.6

DESCRIPTION

A Business Impact Analysis (BIA) is a highly effective tool for developing a BCMS. Organizations can conduct a BIA by surveying key personnel across functional units to determine, from the perspective of their unit, how an outage to key resources will impact the organization's ability to continue operating successfully. Combined with a thorough understanding of the organization's environment and key products and services, the results from conducting a BIA help an organization determine what resources are essential to achieving its critical business functions. This determination is important because it allows the organization to know where to focus its efforts to maintain and improve business continuity.

A risk assessment similarly analyzes an organization for vulnerabilities to its business operations. In this case, the emphasis is on identifying risks that may disrupt the organization's most critical activities and the resources needed to support those activities. After evaluating these risks, the assessment produces a list of the risks the organization should address.

Business Continuity Plans

Primary Function	Identifies and prioritizes resources with the most impact on critical business operations so that an organization can take steps to plan for and address them.
Clause of Origin	**CLAUSE 8.2** The organization shall: **a)** implement and maintain systematic processes for analyzing the business impact and assessing the risks of disruption; **b)** review the business impact analysis and risk assessment at planned intervals and when there are significant changes within the organization or the context in which it operates.
Related Clauses	6.2 7.3 8.3, 8.4, 8.6

DESCRIPTION

A business continuity plan is the key tactical documentation available to employees in a functional unit. As the most specific and technical document in a BCMS, team members turn to their business continuity plan to understand what to do during a disruption. As such, the plan contains specific steps for identifying and categorizing the disruption appropriately, so that employees have the guidance they need to properly assess the issue and escalate it if necessary. Industry best practice is to categorize disruptions by impact level, often with the assistance of a Business Impact Analysis (BIA), and define which levels should be escalated to top management or another team. In addition, a business continuity plan must detail specific procedures for managing the effects of a disruption so that the organization can continue to operate as effectively as possible.

To implement business continuity plans, an organization should first decide how to organize them. Many businesses divide their business continuity plans by functional unit so that each team has its own plan to rely on. Depending on the nature and size of the business, these functional units can be defined as departments, teams, or other appropriate groupings, as long as their personnel share common needs, resources, and responsibilities.

After deciding on functional units, an organization defines specific business continuity objectives to aim for during a disruption. These objectives should be determined by considering the needs of each unit, often drawing on the results of a BIA.

Next, each unit brings this information together to lay out a step-by-step, detailed business continuity plan. Industry best practice is to store multiple backups of these plans to ensure their availability while centralizing them so that team members have the most updated copy at any time. As with other documents, access should be granted to the relevant parties so that they can retrieve business continuity plans when needed.

Finally, an organization is responsible for testing its business continuity plans. This includes each business unit's plan and general, organization-wide plans. See later sections regarding testing and review for further details.

Records of Testing

Primary Function	Demonstrates implementation of a regular plan for validating the business continuity plans and documentation through various exercises and tests, such as tabletop exercises.
Clause of Origin	**CLAUSE 8.5** The organization shall implement and maintain a programme of exercising and testing to validate over time the effectiveness of its business continuity strategies and solutions.
Related Clauses	8.4 8.6 9.1 9.3

DESCRIPTION

Records of testing are documents that show that an organization has been taking appropriate steps to test and validate its business continuity plans. ISO 22301 does not designate a specific media or format for fulfilling this requirement. Instead, it only requires that the records show testing that is aligned with the requirements of Clause 8.5. In other words, the testing program should be based on relevant scenarios with defined objectives and test the participating personnel's ability to respond effectively according to their roles. For example, industry-standard practice is to conduct tabletop exercises, where personnel act out their roles and responsibilities in a simulated situation while being prompted by an exercise leader or third party. Best practice is to conduct these exercises yearly at a minimum, rotating between each business continuity plan or document so that all are validated.

Records of Business Continuity Documentation Review

Primary Function	Demonstrates implementation of a process for regular review and continual improvement of the BCMS, which includes monitoring, measuring, and analyzing it.
Clause of Origin	**CLAUSE 9.3.1** Top management shall review the organization's BCMS, at planned intervals, to ensure its continuing suitability, adequacy, and effectiveness.
Related Clauses	9.1 9.3.2-9.3.3 10.1, 10.2

DESCRIPTION

Records of business continuity documentation review are documents that show that an organization has been making appropriate efforts to review and improve its BCMS. These records are distinct from records of testing because they encompass the whole management system, not just the business continuity plans and controls. Records of testing may be included within the broader records of business continuity documentation review, but are typically accompanied by information related to other clauses such as revisions to the scope or performance evaluation processes.

ISO 22301 expects an organization to "retain documented information as evidence of the results of management review" and "take appropriate action relating to those results" (Clause 9.3.3.2). Thus, these records should indicate management's decisions to make changes to the BCMS such as updates to the scope, modifications to the business continuity strategies, and adjustments to the way controls are evaluated and measured. Furthermore, 22301 expects an organization to continually identify and address non-conformities as part of a continual improvement process. This means an organization should not develop its BCMS once and never return to it. Rather, it is expected to review and update its BCMS regularly because its environment, context, needs, and structure all change over time. To align its BCMS with current needs and abilities, an organization should participate in managerial reviews and take corrective actions on any non-conformities discovered. These non-conformities can be either failing to meet the requirements of ISO 22301, or failing to put its own BCMS into practice.

Internal Audit

Primary Function	Determines if the BCMS is being implemented and maintained in accordance with the organization's needs and requirements and those of the ISO 22301 standard. This is accomplished through planning, performing, and reviewing regular audits of the organization's BCMS.
Clause of Origin	**CLAUSE 9.2.1** The organization shall conduct internal audits at planned intervals to provide information on whether the BCMS: **a)** conforms to: **1)** the organization's own requirements for its BCMS; **2)** the requirements of this document; **b)** is effectively implemented and maintained.
Related Clauses	9.1 9.3 10.1, 10.2

DESCRIPTION

An internal audit is one of the last steps an organization takes on its path to full ISO 22301 compliance. It's a significant effort, which requires an organization to test its BCMS against each line item in 22301, recording all non-conformities to the standard. Additionally, the organization must test the practice of its BCMS (i.e., whether the policies and plans have actually been implemented in the business units themselves). This involves assessing whether all personnel know their roles and responsibilities and whether all plans and solutions are, in fact, capable of supporting critical business functions in a disruption.

To implement internal audits, an organization must first establish an audit program to determine how these audits will be performed. The program must specify how to choose impartial auditors, how frequently to repeat the audit, how to define the audit criteria and scope, and how to document and communicate the results. Once this program has been created, the organization should regularly perform audits based on the defined schedule. The audit results should be documented in an Internal Audit Report so that findings can be reviewed by management and remediated.

Once an organization has conducted its internal audit, it should take appropriate actions based on the findings. This includes reviewing the results, documenting any newly-determined goals and priorities, and making changes to the BCMS as necessary. From there, an organization is ready to conduct its external audit and receive ISO 22301 certification. This is done by hiring one of the handful of ISO 22301 certifying bodies, organizations authorized by ISO to give 22301 certifications. This certifying body will conduct a full audit of the organization's BCMS and, if approved, will award the organization official 22301 certification.

Common Pitfalls

Effective business continuity requires an organization to anticipate, prepare for, and address disruptions of all types and severities. In practice, this looks like a comprehensive and thorough BCMS executing the full range of requirements laid out in ISO 22301. Because this effort covers so much ground and impacts all areas of an organization, it requires in-depth knowledge of both the ISO 22301standard and current industry best practices. Consequently, some organizations struggle to put ISO 22301 into practice.

Based on its deep industry knowledge and extensive experience helping clients comply with ISO 22301, Tevora has identified two common pitfalls that most organizations have difficulty with (1) underestimating time and effort, and (2) inadequate awareness and competence.

Underestimating Time and Effort

The first aspect of ISO 22301 certification that organizations tend to struggle with is properly estimating the amount of time and effort required. Constructing an entire management system like a BCMS is a big project, and many organizations underestimate the amount of work that will be needed.

Developing and implementing an efficient and effective BCMS requires significant energy, resources, and commitment. Many organizations encounter issues when they fail to recognize this and try to get by with only a partial commitment. For example, industry best practice is to reserve at least a year between the start of business continuity efforts (e.g., beginning a gap analysis) and the beginning of the external audit, which is required for certification. This timeline is necessary to allow adequate time for review, analysis, and remediation in between the required steps. Some organizations try to rush this process and fail to implement effective business continuity because they don't leave enough time between steps (e.g., between BIA and internal audit steps). By rushing through steps, these organizations leave no room for the testing and management review phases. As a result, they aren't able to truly validate that their business continuity plans work, which leads to negative consequences down the line, including difficulty passing their external audit.

Another common pitfall organizations experience is failing to allocate adequate time to complete the review and approval steps required for their industry's legal and regulatory obligations (e.g., HIPAA or PCI DSS).

To avoid underestimating the time and effort needed to become ISO 22301-certified, be sure to consider the full extent of work required and the potential pitfalls mentioned in this section. Once you have established a realistic plan and timeline, ensure that you have full buy-in from management and commitments from your team members to conduct the substantial amount of work required.

Inadequate Awareness and Competence

Another common pitfall encountered by organizations seeking ISO 22301 certification is a lack of detailed knowledge of this complex standard and competence in implementing it. Organizations will need to have multiple experts available to their teams with in-depth knowledge of ISO 22301 requirements and extensive experience implementing and maintaining it in similar organizations. Organizations that don't currently have this kind of deep expertise in-house should consider engaging a third party, such as Tevora, to augment and train their teams.

Without this level of expertise, organizations often fail to:

- **Comply** with detailed aspects of the ISO 22301 standard.
- **Create** proper corrective action plans.
- **Meet** legal and regulatory requirements for the organization's industry.
- **Develop** high-quality documentation that addresses the extensive ISO 22301 documentation requirements.
- **Produce** adequate documentation to ensure continuity in the event of management or staff turnover.

Ultimately, these pitfalls can prevent an organization from achieving ISO 22301 certification or greatly increase the time and effort required.

Conclusion

Though arduous and time intensive, the journey to ISO 22301 compliance is well worth the cost for any organization seeking to be resilient in the face of disruptions. In our increasingly interconnected world, with expectations of high availability up and down supply chains and continually escalating cyber threats, having rock-solid business continuity has become table stakes for most organizations. To address this need, organizations should dedicate the time and resources necessary to implement effective business continuity and meet ISO 22301 requirements.

More information and additional ISO resources can be found online on ISO's official website. And as industry experts with ISO 22301-certified lead auditors on our staff—and being ISO 22301 compliant ourselves—Tevora is happy to answer any questions you may have or work with you to help bring your organization into compliance with this important standard. Please feel free to reach out to us through the contact information below.

Author Profile

JONATHAN LEE, Information Security Associate

PRIMARY ROLE

Jonathan is an associate working in the Business Continuity and Disaster Recovery practice under the Privacy, Enterprise Risk, and Compliance (PERC) tower at Tevora. Jonathan assists with evidence review, report writing, and other aspects of assessments within the BCDR practice.

NOTABLE ACCOMPLISHMENTS

Jonathan has recently started his journey into cyber security and BCDR. He has an interest in Disaster Recovery along with Cloud and Web application cyber security. Jonathan graduated from UC Irvine with a Bachelor of Science in Computer Science, with a specialization in Networked Systems, and is also pursuing CISSP certification. In his free time, he enjoys working on security-based coding projects to improve his knowledge of the field.

CERTIFICATION AND TRAINING

B.S Computer Science, UC Irvine

TENURE

Jonathan has been with Tevora since April 2022.

About Tevora

Tevora is a leading management consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. We offer a comprehensive portfolio of information security solutions and services to clients in virtually all industries and also serve institutional and government clients.

Our team has in-depth knowledge of the ISO 22301 standard and years of experience helping clients design and implement business continuity solutions. As an approved ISO 22301 lead auditor, we are well qualified to help your organization become certified for this comprehensive standard.

Tevora's leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability, and our solutions are designed to enhance both.

As a consulting firm that can fully implement whatever it recommends, Tevora works with all of the industry's top vendors yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients' needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as "obsessive." We consider this a fair assessment.

Our hard work and dedication have established us as a reliable partner CTOs, CIOs, and CISOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information, please visit tevora.com.

Our team is ready to discuss your specific challenges and identify the best solutions.

Give us a call at (833) 292-1609 or email us at sales@tevora.com.

TEVORA™

Go forward. **We've got your back.**