

内部情報セキュリティ監査チェックリスト 2013 年版

規格要求事項 (4.1 組織及びその状況の理解)	インタビュー等サイト(現地)確認	確認の有無	不適合の有無	備考(メモ)
<p>組織は、組織の目的に関連し、かつ、その ISMS の意図した成果を達成する組織の能力に影響を与える、外部及び内部の課題を決定しなければならない。</p> <p>注記 これらの課題の決定とは、JISQ31000:2010の5.3に記載されている組織の外部状況及び内部状況の確定のことをいう。</p>	<p>「決定した外部及び内部の課題を説明してください」</p> <p>外部環境</p> <ul style="list-style-type: none"> ・社会の環境(景気、法律の変更、消費者保護の増進、IT 技術の進歩)を考慮しているか。 ・組織間の競合環境(コスト削減、海外進出、海外企業の参入、企業間競争の激化)を考慮しているか。 ・組織の目的に影響を与える主要な原動力及び傾向(地球環境問題への対応、循環型社会への対応)を考慮しているか。 ・外部ステークホルダとの関係及び外部ステークホルダの認知及び価値観(不買運動、人格権侵害、消費者の賠償意識の高揚、消費者の環境保護意識の高揚)を考慮しているか。 <p>内部環境</p> <ul style="list-style-type: none"> ・組織体制、役割及びガバナンス(説明責任が問われる社会に関する無自覚、外部環境の変化に関する無自覚、コーポレートガバナンスの未確定、内部統制の周知徹底不足)を考慮しているか。 ・方針、目的及びこれらを達成するために策定された戦略(事業の国際化、新規事業への展開、資産・利益の減少、社会的責任の積極的対応)を考慮しているか。 ・資源および資本、時間、人員、プロセス、システム、技術(技術革新による安全・環境管理の変化、効率的生産・販売、新技術による商品欠陥、公害への対応)を考慮しているか。 ・情報システム、情報の流れおよび意思決定システム(情報漏洩、情報セキュリティの不完全、新システムの参入)を考慮しているか。 			

見本

内部情報セキュリティ監査チェックリスト 2013 年版

規格要求事項 (10.2 継続的改善)	インタビュー等サイト(現地)確認	確認の 有無	不適合 の有無	備考(メモ)
<p>組織は、ISMS の適切性、妥当性及び有効性を継続的に改善しなければならない。</p>	<p>「ISMS の継続的改善のための活動はどのようなものがありますか」 ・各活動は、継続的改善を行っているか。</p>			

要求事項については、「JISQ27001 : 2014 情報セキュリティマネジメントシステム—要求事項」からの引用です。

内部監査チェックリスト(情報セキュリティISMS／ISO27001:2013)

この度は、内部情報セキュリティ監査チェックリストサンプルのご覧頂きましてありがとうございます。

この他に、内部品質監査チェックリストサンプル、内部環境監査チェックリスト、内部個人情報保護監査チェックリスト、内部労働安全衛生監査チェックリスト、内部苦情対応監査チェックリストもご紹介します。

<http://www.isonavi.net/tools/checklst.html>

をご覧ください。