令和5年度

札幌市情報セキュリティ内部監査支援業務

仕様書

1. 業務名称

令和5年度 札幌市情報セキュリティ内部監査支援業務

2. 業務期間

契約締結日から令和６年３月22日（金）まで

3. 業務の概要

本市では、「情報セキュリティポリシー（以下「セキュリティポリシー」という。）」に基づき実施している情報資産の管理、各種業務システムの保守・運用及び職員研修等の情報セキュリティ対策の向上に資することを目的として情報セキュリティ内部監査（以下「内部監査」という。）を行っている。

本業務は、本市担当者が基準等に準拠した、適切な内部監査を実施できるよう支援を行うものである。

4. 発注部署

札幌市デジタル戦略推進局情報システム部システム調整課

連絡先：〒003-0801 北海道札幌市白石区菊水１条３丁目 1-5 菊水分庁舎

電話番号：011-826-6479　FAX：011-813-2185

5. 履行場所

主な履行場所は「札幌市白石区菊水１条３丁目 1-5（札幌市菊水分庁舎）」とする。

また、実地検査（ヒアリング）等は本市が別に認めた場所（札幌市内）で行うものとする。

なお、来庁又は本市職員の立会を要しない作業については、この限りではない。

6. 業務内容

本市が、令和４年度に実施した内部監査の結果より、本市担当者と課題点等の洗い出しを行う。その内容を踏まえ、効率的かつ回答者の負担を軽減した内部監査実施手順書、調査票の検討及び案の作成を行い、本市担当者が実施する内部監査の支援を行う。

なお、各資料の作成は、作成案をもって本市と協議を行い、承認を得るものとする。

(1) 内部監査実施手順書及び調査票の案の作成

ア　別紙1「情報セキュリティ内部監査実施要領」の実施概要に掲げられる①～③の項目について、具体的な手順を標した実施手順書及び調査票の案を作成すること。

※調査票は、本市と協議の上、入力フォーム等のツールを用いても構わない。

なお、クラウドサービス等外部のツールを使用する場合は、受託者にて集計を行うこと。

イ　情報セキュリティに明るくない職員が使用することを想定し、実施手順書や調査票等の対象者に配布する資料においては、平易かつ詳細に記載すること。

また、必要に応じて専門用語を解説した用語集等を作成すること。

(2) 現地ヒアリングの支援

ア　本市が選定する部署、システム及びCISO承認に対し、本市担当者と現地へ訪問して実地検査（ヒアリング）を実施すること。

※対象数は別紙1「情報セキュリティ内部監査実施要領」の対象範囲を参照

イ　「８．監査人の要件」に掲げる条件を満たす監査人が１名以上現地にいること。

ウ　ヒアリングを実施した部署については、監査結果一覧を作成すること。

(3) 内部監査の結果の分析

別紙1「情報セキュリティ内部監査実施要領」の実施概要に掲げられる①～③の結果を集計し、その監査結果の分析を行うこと。

(4) 監査報告書の作成及び説明会の実施

(3)の分析結果を基に報告書を作成し、本市担当者に対し説明を行うこと。

なお、報告書には、監査結果に基づく提案等も含むこと。

7. 監査基準

(1)札幌市情報セキュリティポリシー（基本方針及び対策基準）

(2)情報セキュリティ技術対策基準

(3)情報セキュリティ実施手順

(4)札幌市情報セキュリティ監査実施要領

(5)地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）

(6)地方公共団体における情報セキュリティ監査に関するガイドライン（総務省）

(7)上記のほか委託期間において情報セキュリティに関し有用な基準等で、本市と協議

して採用するもの

8. 監査人の要件

(1)受託者は情報セキュリティサービス基準適合サービスリスト（うちセキュリティ監査サービスに係る部分）に登録されていること。

(2)業務責任者は、情報セキュリティ監査に必要な知識及び経験（地方公共団体における情報セキュリティ監査の実績）を持ち、次に掲げるいずれかの資格を有する者を選任すること。

ア システム監査技術者

イ 公認情報システム監査人（CISA）

ウ 公認システム監査人

エ ISMS 主任審査員

オ ISMS 審査員

カ 公認情報セキュリティ主任監査人

キ 公認情報セキュリティ監査人

(3)業務責任者及び担当者が、監査対象となる情報資産の管理及び当該情報資産に関する情報システムの企画、開発、運用、保守等に関わっていないこと。

9. 提出書類

受託者は、下表に定める書類を本市に提出すること。

また、そのほか本市で必要とするものについては、その都度提出すること。

提出書類	部数	提出時期	備考
① 業務責任者指定通知書	1部	業務着手時	「8. 監査人の要件」を満たすことが確認できる書類の写しを添付すること。また、業務期間中に業務責任者を変更するときは、速やかに届け出ること。
② 履行管理体制図			業務期間中に履行管理体制を変更するときは、速やかに届け出ること。
③ 内部監査の集計結果及び実施報告書 ④ 実施報告書のダイジェスト版	1部	業務完了時	

⑤ 本件業務で使用した資料、書類、議事録等			
⑥ その他、本市が別に必要と定めるもの	必要数		
⑦ “①～⑥”の電子データ（CD-R 又は DVD-R）	１部		電子データは、Microsoft Word、Microsoft Excel 、 Microsoft PowerPoint 及び PDF を基本とする。

※指定期限までの提出が困難な場合、予め提出可能な期限を提示し、本市の了承を得ること。また、この場合においては期限を厳守すること。

10. 成果物の帰属

成果物及びこれに付随する資料は、全て本市に帰属するものとし、書面による本市の承諾を受けないで他に公表、譲渡、貸与又は使用してはならない。ただし、成果物及びこれに付随する資料に関し、受託者が従前から保有する著作権は受託者に留保されるものとし、本市は、本業務の目的の範囲内で自由に利用できるものとする。

11. 環境に対する配備

(1)受託者は、本市の環境マネジメントシステムに準じ、環境負荷低減に努めること。

(2)電気、水道、油、ガス等の使用にあたっては、極力節約に努めること。

(3)ごみ減量及びリサイクルに努めること。

(4)両面コピーの徹底やミスコピーを減らすことで、紙の使用量を減らすよう努めること。

(5)自動車等を使用する場合は、できるだけ環境負荷の少ない車両を使用し、アイドリングストップの実施など環境に配慮した運転を心がけること。

(6)業務に係る用品等は、札幌市グリーン購入ガイドラインに従い、極力ガイドライン指定品を使用すること。

12. 委託業務の留意事項

業務の実施にあたっては、以下の事項に留意する。

(1)監査実施計画書の提出

契約締結後、受託者は監査実施計画書を提出し、市及び受託者の協議により委託

業務の詳細内容及び各作業の実施時期を決定するものとする。

(2)資料の提供等

本業務の実施にあたり、必要な資料及びデータの提供は本市が妥当と判断する範囲内で提供する。なお、受託者は、本市から提供された資料は適切に保管し、特に個人情報に係るもの及び情報システムのセキュリティに係るものの保管は厳格に行うものとする。また、契約終了後は本件監査にあたり収集した一切の資料を速やかに本市に返還し、又は破棄するものとする。

(3)再委託

原則として、本業務の全部又は一部を第三者に委託（以下「再委託」という。）してはならない。止むを得ず再委託を行う場合は理由及び範囲を明確にし、事前に本市の承認を得ること。

(4)秘密保持義務

本業務で知り得た情報及び入手したデータは、本契約の履行期間及び履行後においては第三者に漏らしてはならず、本業務に関わる従業員その他関係者にも周知徹底しなければならない。

データを取り扱うときは、これを流出させないように留意しなければならない。特に、次に掲げる各号を遵守すること。

ア　本市の情報を目的外に使用しないこと。

イ　本市の情報を複写、複製する場合には本市の許可を事前に得ること。

ウ　本市の情報を外部記憶媒体等で持ち出す場合は、紛失及び盗難を避けるため厳重に保管すること。また、データは必ず暗号化をすること。

エ　本市の情報を取り扱う際は、のぞき見等への対策を行い、関係者以外に情報が知れ渡らないようにすること。

(5)議事録等の作成

受託者は、本業務の実施にあたり本市と行う会議、打ち合わせ等に関する議事録を作成し、本市にその都度提出して内容の確認を得るものとする。

(6)関係法令の遵守

受託者は業務の実施にあたり、関係法令等を遵守し業務を円滑に進めなければならない。

(7)報告等

受託者は作業スケジュールに十分配慮し、本市と密接に連絡を取り業務の進捗状況を報告するものとする。

13. その他特記事項

(1)交通費その他諸経費は本業務による費用に含まれており、別途支給することはないので注意すること。

(2)ISMS、関連情報の最新動向、コンサルティングのノウハウを活用し、企画・提案を行うこと。

(3)成果物の納入後、その内容が要求品質を満たしていないものについては、受託者の責任において関連する項目を再検査し、当該個所の修正を行うこと。

(4)契約図書に定めのない事項及び疑義が生じた場合は、業務担当者と協議をするものとし、その内容を記載した議事録を提出すること。

情報セキュリティ内部監査実施要領

1. 実施方針

内部監査の実施方針は以下の３点とし、助言型監査とする。

(1) ポリシーに基づく対策の実施状況の確認

ポリシーに規定される各項目が遵守されているかをチェックし、必要に応じて改善提案を行う。

(2) 情報資産の取扱状況の確認

情報資産（個人情報、機密情報等）の取扱状況の実態（一覧の作成状況等）をチェックし、必要に応じて改善提案を行う。

(3) 緊急時の連絡・報告体制の整備状況の確認

情報システムを利用する業務において、緊急時の連絡・報告体制等の必要資料が整備されているかをチェックし、必要に応じて改善提案を行う。

2. 実施概要

各所属は、配布される内部監査実施手順書等に従い、内部監査を実施する。

内部監査の実施項目は以下の３点とする。

実施項目	備考
① 自己点検	「１　実施方針」に掲げる(1)～(3)の状況について、各所属が自身で確認を行い、その結果を 3 種類の調査票（所属、職員及びシステム）に記入する。 確認は、所属、職員及びシステムの各単位で行う。
② 相互点検	「１　実施方針」に掲げる(1)～(3)の状況を客観的に評価するため、調査票を基に所属相互で点検を行う。 原則として同一部内の課単位で実施する。ただし、事務室の都合等により実施が困難な場合は、係単位等での実施を可能とする。
③ 実地検査（ヒアリング）	「１　実施方針」に掲げる(1)～(3)の状況を客観的に評価するため、情報システム部が実施するヒアリングを受ける。実地検査では、自己点検の内容を基に詳細の聞き取り及び必要に応じて改善提案が行われる。

3. 対象範囲

内部監査のうち、自己点検及び相互点検は、本市における全ての所属（課等）、職員及びシステムを対象に実施する。ただし、実地検査の対象は、相互点検を省略する。

実地検査は、所属、システム及び CISO 承認について実施する。CISO 承認は、本市が一部を抽出したものについて検査を行う。

※CISO 承認とは、札幌市情報セキュリティポリシーに基づく CISO の承認が必要な案件

のことを指す。

各数量は概ね次に掲げるとおりである。

(1) 所属数　約 500

(2) 職員数　約 15,000

(3) システム数　約 300

(4) 実地検査の実施数　約 50

業務責任者指定通知書

令和　　年　　月　　日

（あて先）札幌市長

受託者（住所）
（氏名）　　㊞

件　　名　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

上記業務に係る業務責任者等について、次のとおり定めたので通知します。

区分	氏名	備考（資格等）
業務責任者		