情報セキュリティ外部監査業務調達仕様書

1　業務名

情報セキュリティ外部監査業務

2　目的

本市では令和７年４月１日現在、業務を実施するにあたり各室課が主体となって導入した118に及ぶ情報システムを運用している（外部サービス利用を含む）。

これらの運用にあたり、吹田市情報セキュリティポリシーが遵守されていることを確認するため、定期的に情報セキュリティ監査を実施しており、令和５年度からは、外部の専門家の客観的・専門的な知見を活用すべく、外部監査を実施しているところである。

本業務は、令和８年度以降も引き続き、外部の専門家による主要な監査対象システムに対する監査を実施するとともに、外部の専門的な知見の活用によりセキュリティを担保することを目的とするものである。

3　発注部署

行政経営部デジタル政策室

4　履行期間

令和８年７月１日から令和11年３月31日まで

5　業務概要

本市が運用する情報システムに対し情報セキュリティ監査を実施することで、本市情報セキュリティポリシーに基づき適切に管理及び運用されているかどうかを点検し、セキュリティの向上を図る助言型の情報セキュリティ監査とする。

本市が所管するシステムは住民情報系、内部事務系、独自事務系を合わせ令和７年４月１日時点で118システムあり、今後も新規導入により増え続ける見込みである。

本業務では、それらの中の主要なシステムに対し、年間15システムの監査を実施することとする。なお、各年度の監査対象システムについては当該年度の当初(令和８年度にあっては契約締結後速やか)に、過去の監査実績やその他本市セキュリティに係る事情等を考慮して決定するものとする。

想定する監査システム数は以下のとおりとする。

・令和８年度　15システム
・令和９年度　15システム
・令和10年度　15システム

6　情報セキュリティ外部監査業務の詳細

当該業務の詳細を以下に示す。

（1） 監査手順

ア　監査計画

当該年度の監査対象システムを決定し、実施計画を策定する。その後、CISOにおいて承認を受ける。

イ　監査準備

監査を受ける部署とのスケジュール調整を行い、事前アンケート（予備調査）を実施する。また、回答結果から監査項目を決定しヒアリングシートを作成する。

ウ　監査実施

現地調査及びミーティングを行う。

エ　フォローアップ実施

前年度までの監査でフォローアップが必要とされた案件につきフォローアップを実施する。なお、令和 8 年度は令和 7 年度以前の残案件につきフォローアップを行うこと。残案件は 19 システム 66 件で、内容は「ID の管理・事業者からの報告書徴取・手順書の整備」などであり、案件の詳細は契約締結後に事業者に交付する。

オ　監査報告

監査報告書を作成し、CISO に報告する。

（2）委託内容

ア　監査計画

・監査対象システム選定に係る支援
・実施計画書の作成

イ　監査準備

・事前アンケート項目の作成
・事前アンケート回答結果の集計
・ヒアリング項目の決定及びヒアリングシートの作成

ウ　監査実施

・現地調査及びミーティングの実施
・監査結果に基づくフォローアップ

エ　監査報告

・監査報告書の作成及び CISO への報告

オ　デジタル政策室職員への監査実施に係る教育、ノウハウ共有等

・職員の ICT 教育の一環として非常に重要視している。本業務終了後も職員が

独力で監査ができるように支援すること。

・職員による内部監査を実施するにあたっての点検用チェックリストの作成や、報告書様式の作成支援

カ　その他

・本市との協議参加

・その他本業務における手法、改善等にかかる提案

・その他類似監査業務との役割整理、改善等にかかる提案

・前年度に改善事項があったシステムについての後追い

（３）納品物

以下に該当する物をそれぞれ書面及びデータで納品すること。なお、アの監査報告書本体は、詳細版と概要版とに分けて作成すること。また、納品する成果物に関する権利は、本市に帰属するものとする。

ア　監査報告書

イ　脆弱性検出一覧

調査結果から運用管理上の脆弱点となる事項を取りまとめたものであること。

ウ　改善方法一覧

脆弱点と判断された項目について、採るべき改善策を取りまとめたものであること。

エ　手順書等

内部監査を容易に実施することを可能とするための手順書、様式等

7　監査人要件

情報セキュリティ外部監査に係る監査人要件として、次の（１）から（３）の要件をすべて満たしていること。

（１）監査は、監査責任者（１名）、監査人（数名）による監査チームを編成し実施すること。

（２）監査チームには、以下に定める資格又は同等のものを有している者が、１名以上含まれていること。

ア　公認情報セキュリティ監査人

イ　公認システム監査人

ウ　CISA: Certified Information System Auditor

エ　システム監査技術者試験に合格

（３）監査チームには、情報セキュリティ監査、システム監査、情報セキュリティコンサルティング、情報セキュリティポリシー作成支援のうちのいずれかの実務経験を有する者が、１名以上含まれていること。

（４） 契約締結後速やかに、監査チームの体制図等、監査人要件を満たしていることが確認できる書面を提出すること。