{customer}

Gap Assessment Executive Summary

Table of Contents

Introduction

TPx conducted a Cybersecurity Gap Assessment on behalf of {customer}. This engagement was designed to evaluate {customer}'s security program in a variety of areas, with the goal of providing {customer} with a summary of (a) their current ability to defend their organization against cyberthreats; (b) their ability to maintain a level cyberdefense moving forward; and (c) a list of actionable items that they can perform to increase their security posture and reduce overall risk to the organization. The primary TPx Consultants for the assessment were {consultant 1} and {consultant 2}.

This document serves as the contract Deliverable *Executive Summary Report*, as specified in the Statement of Work outlining the work scope for this engagement. It provides the results of the detailed investigation into the customer's security environment, as well as a list of recommended next steps for {customer} to undertake to further mature their security footprint.

Documents Provided

The following documents are the contract deliverables for the gap assessment.

{customer} - Gap Assessment Heatmap.pdf

> Provides a "heatmap" of the NIST 800-171 standards that are applicable to gap assessments. Each item is rated on a scale of 0 to 5 as indicated above.

{customer} - Gap Assessment Interviews.pdf

> Lists questions and responses received during interviews conducted to obtain additional information or clarification.
>
> This document is in the same sequence as the heatmap.

{customer} - Gap Assessment Project.pdf

> Documents the project status.

{customer} - Gap Assessment Report.pdf

> Contains the complete results of the gap assessment, including statistics, recommendations, and for each topic in the heatmap: rating, findings, best practices, and recommendations.
>
> This document is in the same sequence as the heatmap.

{customer} - Gap Assessment Summary.pdf

> Provides a high-level Executive Summary of the results of the Gap Assessment.

Heatmap Summary

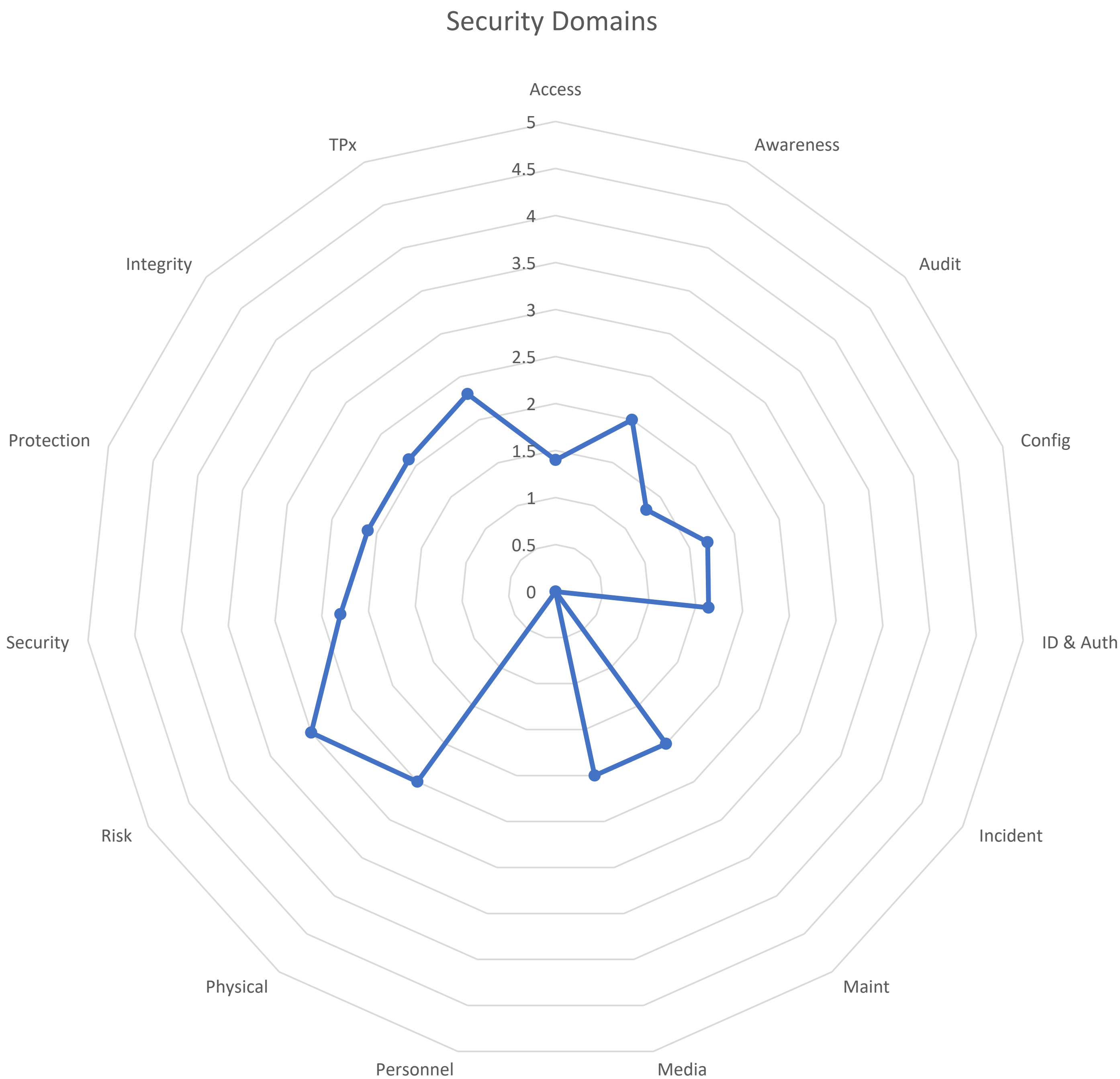
Overall Security Program Score

(2) - Developing

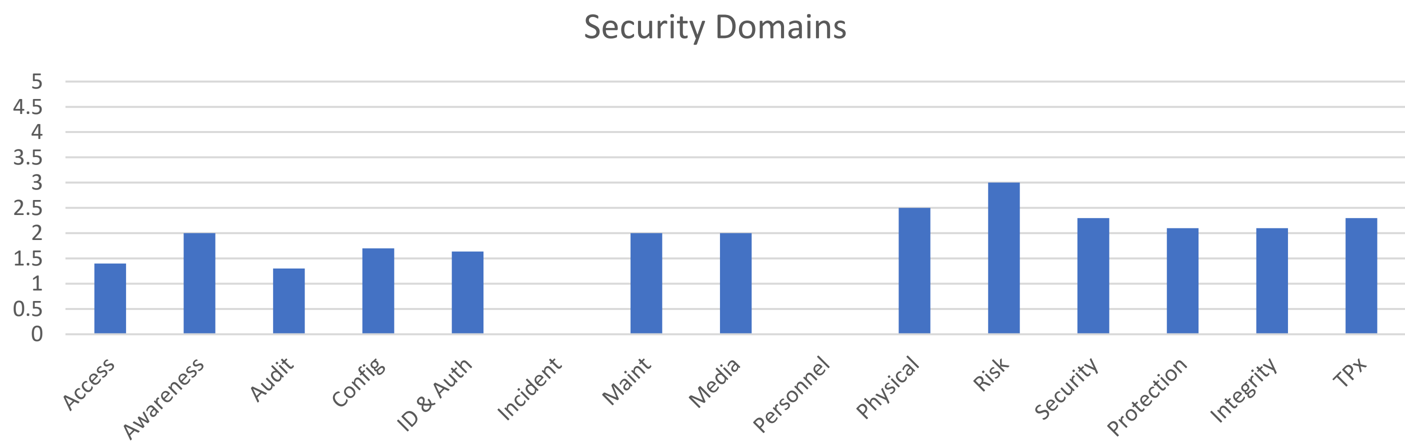
Developing information security requirements, practices, controls and/or documentation that translate into repeatable results.

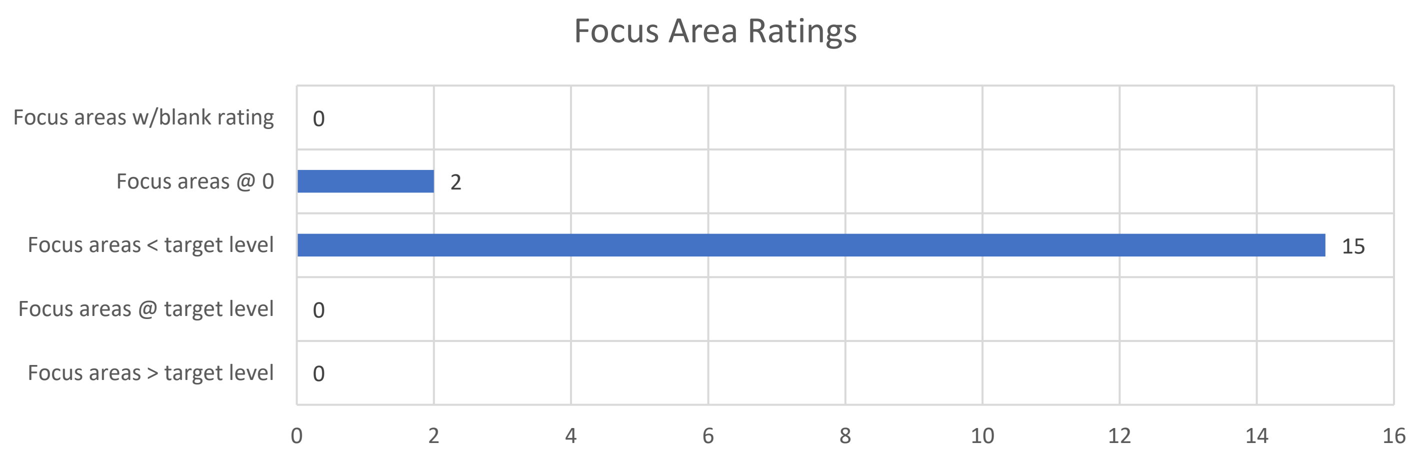
Security Domain Ratings

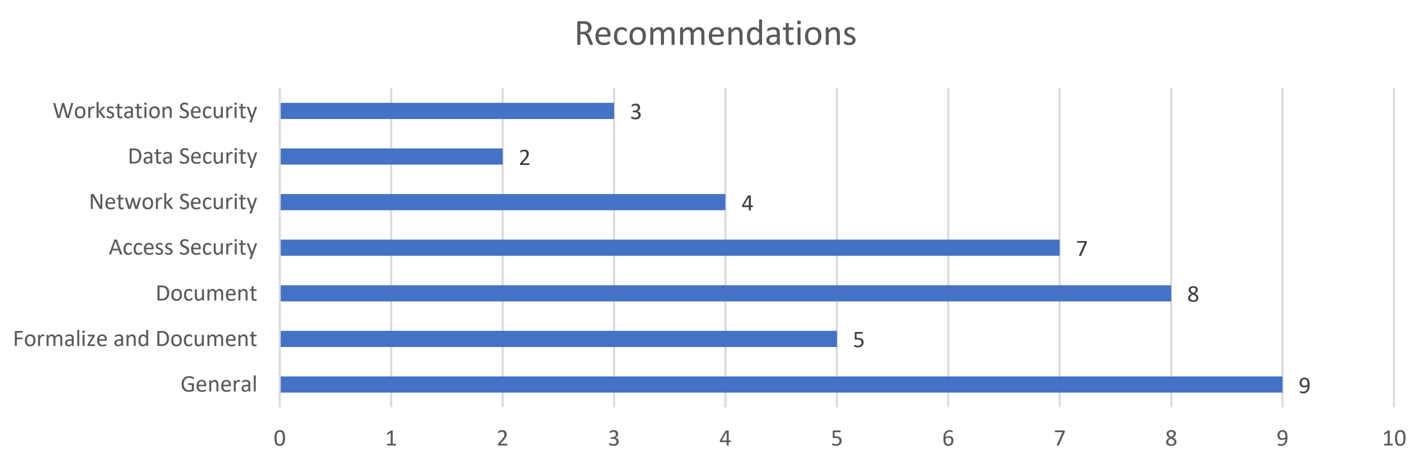
Security Domains	Assessor Rating	Target Level	Risk Gap
Access Control	1.4	5	-3.6
Awareness and Training	2.0	5	-3.0
Audit and Accountability	1.3	5	-3.7
Configuration Management	1.7	5	-3.3
Identification and Authentication	1.6	5	-3.4
Incident response	0.0	5	-5.0
Maintenance	2.0	5	-3.0
Media Protection	2.0	5	-3.0
Personnel Security	0.0	5	-5.0
Physical Protection	2.5	5	-2.5
Risk Assessment	3.0	5	-2.0
Security Assessment	2.3	5	-2.7
System and Communications Protection	2.1	5	-2.9
System and Information Integrity	2.1	5	-2.9
TPx	2.3	5	-2.7
	1.8	5	-3.2


Security Domains
Access
Awareness
Audit
Config
ID & Auth
Incident
Maint
Media
Personnel
Physical
Risk
Security
Protection
Integrity
TPx
5
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0

Statistics


Security Domains
5
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Access
Awareness
Audit
Config
ID & Auth
Incident
Maint
Media
Personnel
Physical
Risk
Security
Protection
Integrity
TPx


Focus Area Ratings
Focus areas w/blank rating
0
Focus areas @ 0
2
Focus areas < target level
15
Focus areas @ target level
0
Focus areas > target level
0
0
2
4
6
8
10
12
14
16


Recommendations
Workstation Security
3
Data Security
2
Network Security
4
Access Security
7
Document
8
Formalize and Document
5
General
9
0
1
2
3
4
5
6
7
8
9
10

High-Priority Recommendations

NIST Domain(s)	Description
3.13.1 3.13.2	Emails are not a secure method for transmitting passwords. Consider alternate methods of providing passwords such as sealed envelope, token, encrypted email, Microsoft Teams, etc.
3.1.6 3.2.7	Wherever possible, replace common IT user id and password with individual user ids and passwords so actions can be traced back to individuals. Document any areas or systems where that is not possible and why.
3.7.4	Implement MFA wherever possible, including VPN and remote network access.
	Migrate to WIFI 6 security as soon as humanly possible.
	Establish and document encryption policy and procedures for mobile devices, including laptops, tablets, smart phones, and any other mobile computing system (laptops are already encrypted, but it’s not documented).

Full list of recommendations is available in the document {customer} – Gap Assessment Report.pdf.

Appendix A - Methodology

TPx reviewed {cust abbr}'s security program through interviews, policy review, validation, and investigation of processes. For each focus area, the relevant policy & process documents were read and evaluated based on thoroughness, clarity, applicability to task, and alignment with National Institute of Standards and Technology (NIST) standards. Follow-up questions were then developed where necessary, and the relevant points of contact were interviewed to provide clarity and further information to the material covered in the document(s). Where possible, the technical implementation of the baseline controls was also observed and evaluated, providing insight into the execution of the defined security policies and processes.

Following the steps above, each subcomponent within a given focus area was rated on a zero to five scale with respect to the criteria outlined above. The six ratings levels are as follows:

- **Maintaining (5)** Managed information security whereby generated metrics are applied to the performance evaluation and continuous improvement of information security.
- **Managed (4)** Defined information security established that generates relevant, measurable, and useful metrics.
- **Documented (3)** Well-established information security requirements, practices, controls, and documentation that translate into consistent repeatable and predictable results.
- **Developing (2)** Developing information security requirements, practices, controls and/or documentation that translate into repeatable results.
- **Minimal (1)** Early reactive information security requirements, practices, inadequately controlled and/or documented.
- **None (0)** No information security requirements, practices, controls, or documentation.

These ratings are then aggregated across all subcomponents within each focus area, to compute an area-level rating. Finally, the area-level ratings are aggregated to provide a program-wide rating that takes into account all aspects of the customer's security program that were within the work scope of the engagement.

In each case, the subcomponent is also assigned a "target" rating level. This target represents the desired level of maturity for that subcomponent. While a 100% secure environment is desirable, it is also unattainable, due to usability, technical, budget, and other considerations. These target levels reflect the appropriate trade-off between security and these considerations, as determined for the specific environment under assessment. The difference between the target level and observed level for any subcomponent, focus area, or program, represents the "gap" between the observed and desired states.

The ratings and target levels for each subcomponent and focus area are contained in a heatmap document that accompanies this report. The heatmap enables quick identification of the subcomponents and focus areas with the largest deviation from target, and which therefore are the most likely candidates for improvement. The report included in this document contains focus area ratings and supporting narrative for each area.