Close the InfoSec Skills Gap: Develop a Technical Skills Sourcing Plan

Systematically source the skills your organization needs.

Info-Tech Research Group, Inc. is a global leader in providing IT research and advice.
Info-Tech's products and services combine actionable insight and relevant advice with
ready-to-use tools and templates that cover the full spectrum of IT concerns.

INFO~TECH
RESEARCH GROUP

Table of contents

ANALYST PERSPECTIVE

Aligning security initiatives skill needs with role requirements is the cornerstone to addressing the cybersecurity talent shortage.

> *Cybercrime is outpacing and outwitting the supply of cybersecurity talent. This has led to a high demand for cybersecurity professionals across all industry verticals.*
>
> *To prepare for the foreseeable challenge, all organizations should proactively compile information from their security strategy and roadmap, and align the skills needed to successfully to execute and maintain the planned initiatives with the current and/or future security roles of the organization. It is only then that a skills gap can be diagnosed and a realistic sourcing plan discussed and created.*

Michelle Tran,
Consulting Analyst, Security, Risk & Compliance
Info-Tech Research Group

Our understanding of the problem

This Research Is Designed For:

✓ IT security leaders

This Research Will Help You:

✓ Identify the technical skills that will be needed to meet your organization’s short- and long-term security initiatives.

✓ Identify technical skill gaps in your organization’s current workforce.

✓ Develop roles that align with your security roadmap.

✓ Create an action plan to acquire skills.

This Research Will Also Assist:

✓ Human resource professionals

✓ CISOs

✓ Chief technology officers

✓ Chief information officers

This Research Will Help Them:

✓ Understand target skills for the future of security teams.

✓ Improve security job descriptions.

✓ Establish a shared lexicon between IT and human resource staff for obtaining, retaining, and training a strong cybersecurity workforce.

Executive summary

Situation

- The demand for cybersecurity talent far exceeds the supply of available professionals. As a result, organizations are struggling to protect their data against the evolving threat landscape.

Complication

- Lack of clarity around the required skills makes finding the right skills difficult.
- Organizations struggle to develop a workforce strategy that aligns with the security roadmap.
- Solving the talent shortage requires proactivity. Organizations must consider future skill requirements to be cyber ready.

Info-Tech **Insight**

1. **Plan for the inevitable.** All industries are expected to be affected by the talent gap in the coming years. Plan ahead to address your organization's future needs.
2. **Base acquisition decisions on the five key factors to define skill needs.** Create an impact scale for the five key factors (data criticality, durability, availability, urgency, and frequency) that reflects your organizational strategy, initiatives, and pressures.
3. **A skills gap will always exist to some degree.** The threat landscape is constantly changing, and your workforce's skill sets must evolve as well.

Resolution

- Organizations must align their security initiatives to talent requirements such that business objectives are achieved and the business is cyber ready.
- Begin by identifying your future state. Identify the needed skills in the organization to support planned projects and initiatives.
- Leverage your security roadmap to identify skills needed in the future.
- Decide how you'll acquire needed skills based on characteristics of need for each skill.

The cybersecurity shortage is here to stay

What is the cybersecurity talent shortage?

The cyber skills shortage is the lack of qualified professionals to fill cybersecurity roles.

1. Not enough people are entering the cybersecurity industry.
2. Current cybersecurity professionals are deficient in the skills required to perform their roles effectively.

The cybersecurity talent shortage is close to **three million** globally.

(ISC)², 2018

Why does the skills gap exist?

- **Breaches are the new norm.** All organizations are viable targets regardless of enterprise size and industry.
- **Sheer volume of threats.** According to ITRC Annual Data Breach Review, from 2016 to 2017 there was a 44.7% upturn of reported breaches (CyberScout, 2018).
- **Companies are unsure of what skills or qualifications are needed.** There has been a lack of investment in developing a security strategy and/or workforce planning.
- **Data breaches are damaging to the organization.** This includes reputational, productivity, and monetary damages.
- **There has been an increase in regulatory and compliance obligations** (e.g. GDPR, PCI-DSS, HIPAA).
- **The threat landscape is evolving.** Organizations are seeking specialists who can offer innovative solutions to combat current and future threats.

The cybersecurity field has a **0% unemployment rate.**

Cybersecurity Ventures, 2016

The shortfall in cybersecurity talent is a major weakness to all organizations

Cybersecurity staff are needed to effectively monitor, plan for, manage, respond to, and recover from cyberattacks.

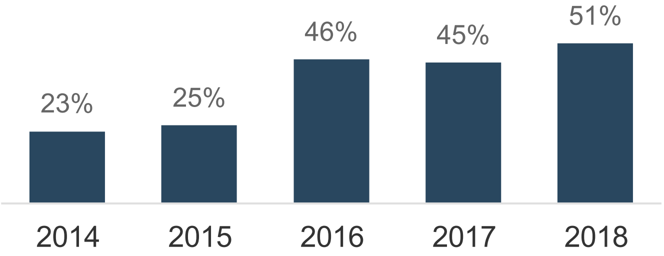
One in three
security professionals say a skills shortage makes their organization more desirable hacking targets.

Source: Enterprise Strategy Group, 2017

One in four
security professionals say their organizations have lost proprietary data as a result of their cybersecurity skills gap.

Source: McAfee, 2016

Percentage of security professionals who claim their organizations have a problematic shortage of cybersecurity skills



Source: Enterprise Strategy Group, 2017; CSO, 2018 *N*=620

❯ **71%** of security professionals believe that a shortage of cybersecurity skills negatively and directly damages the organization (e.g. employee burnout, lack of security planning).

❯ **94%** of security professionals agree that staying current in their skills is necessary to counter the evolving threat landscape.

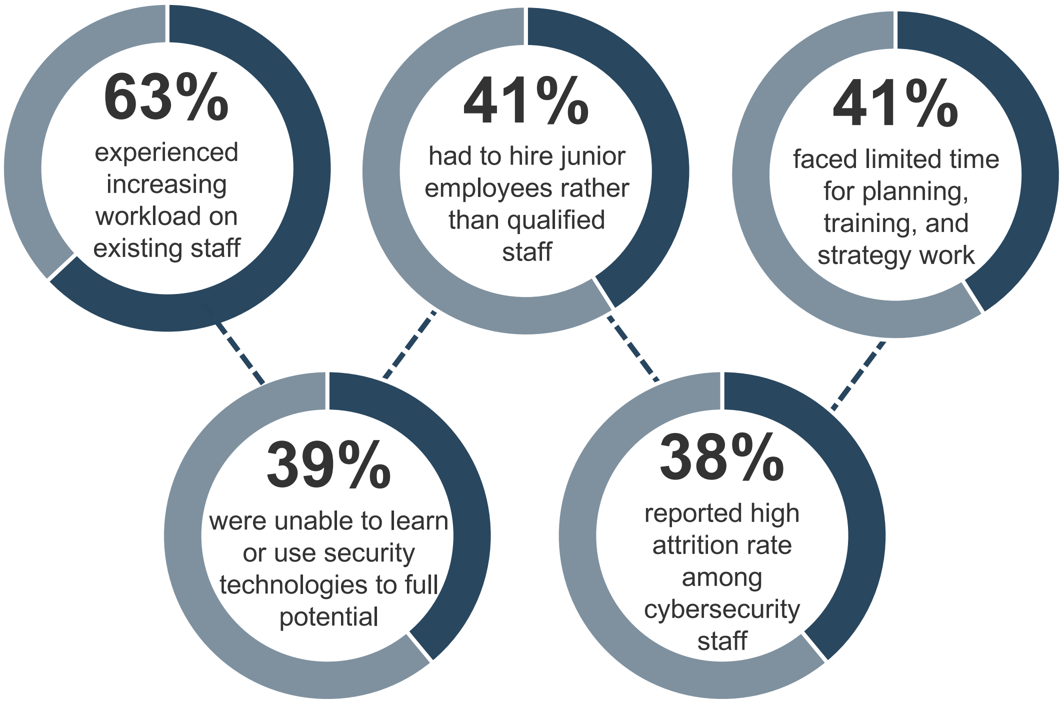
Sources: McAfee, 2016; Enterprise Strategy Group, 2017; CSO, 2018

The skills shortage impacts organizations in many security areas and tasks

Top Contributors to Security Events

1. Lack of adequate training for non-technical employees.
2. Cybersecurity team could not support the size of the organization.
3. Business management treated cybersecurity as a low priority.
4. The existing cybersecurity team could not keep up with workload.

How the Shortage Has Impacted Cybersecurity Professionals



63% experienced increasing workload on existing staff

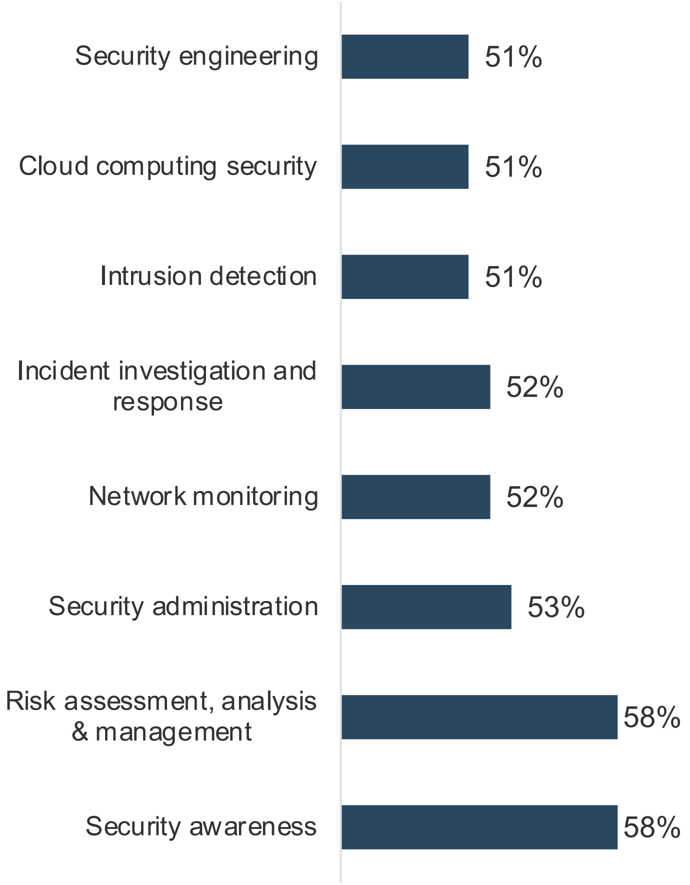
41% had to hire junior employees rather than qualified staff

41% faced limited time for planning, training, and strategy work

39% were unable to learn or use security technologies to full potential

38% reported high attrition rate among cybersecurity staff

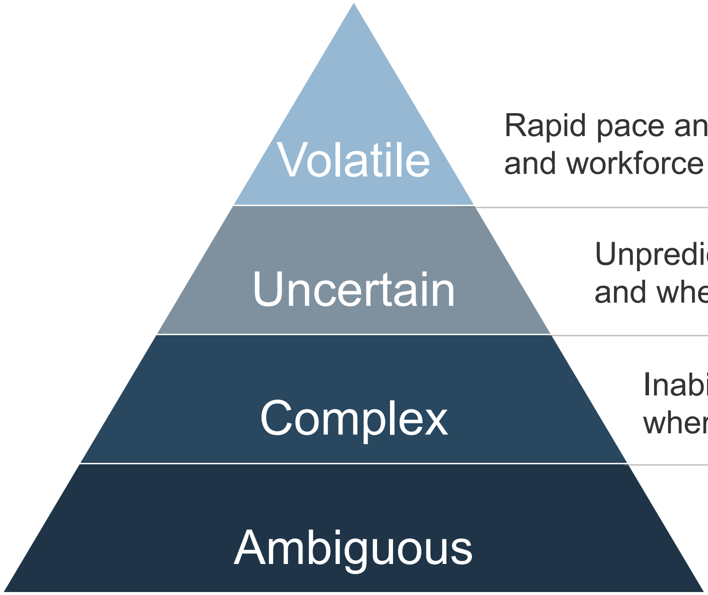
Top Needed Cybersecurity Areas of Expertise



Sources: Enterprise Strategy Group, 2017; ISC^2, 2018

Security *and* business pressures transform the skills needed to manage your environment

A VUCA world requires organizations to keep up with constantly evolving skill needs.



Volatile

Rapid pace and a high degree of change makes predicting and planning for future projects and workforce development difficult.

Uncertain

Unpredictable issues and events make it difficult to know which skills will be required and when.

Complex

Inability to define what skills will be required in the future creates an environment where adaptability, rather than experience, is in demand.

Ambiguous

Connections between skills and desired security and business outcomes are less clear, requiring a greater need to evaluate context for skills application.

- Business strategy must adapt rapidly to keep pace with changes in the business environment.
- Organizational skills must be sufficiently flexible to support rapid change, and there must be processes in place to acquire needed skills.
- Put greater focus on key skills aligned with organizational goals to allow for targeted development efforts, and combat the gaps that may interrupt business operations.

Take a strategic approach to assessing skills and addressing gaps

Info-Tech Insight

Don't be in a state of constant skills shortage with no plan to address it. Look beyond the next project into long-term plans.

- Relying on tactical, reactionary, short-term solutions to resourcing leads to inflexibility and suboptimal outcomes.
- Effectively acquiring skills in a rapidly changing world requires the organization to proactively and strategically assess future skill needs.
- Understand what skills you need to support processes and services in your current and future state environment before you decide how to acquire those skills.

Organizations must plan for:

> “*A **continually changing set of required employee skills** and job duties and a huge gap between the needed and the available skill sets.*”
>
> – Dr. John Sullivan

> “*In the long term, companies need people who can solve multiple problems within their skill sets, and apply skills in multiple tactical ways – but businesses have a tendency to think a quarter at a time.*”
>
> – David Linthicum,
> SVP, Cloud Technology Partners
> Info-Tech Interview

Establish your future skill needs *before* you identify current capabilities for better planning outcomes

Base your skill needs on the strategic requirements of your business and security department.

1 Define Your Future State

Review your security roadmap, initiatives, and strategy.

Identify skills gaps that hinder the successful execution of identified initiatives.

2 Identify Skills Gaps

Inventory your workforce and identify work roles that you intend to obtain in the future.

Adapt the initiative skill gaps identified in the previous step to define the technical skill requirements for current and future work roles.

Conduct a skills assessment on your current workforce to identify employee skill gaps.

3 Decide Whether to Build or Buy Skills

Take action to address gaps, mitigate risks, and deliver projects and initiatives.

For current roles with skill gaps, develop an action plan.

For future roles, decide whether to train, hire, contract, or outsource each skill based on the level of impact across the five key skill need factors.

Info-Tech **Insight**

Plan for the inevitable. All industries are expected to be affected by the talent gap in the coming years. Plan to address the skills required for the future state of your organization.

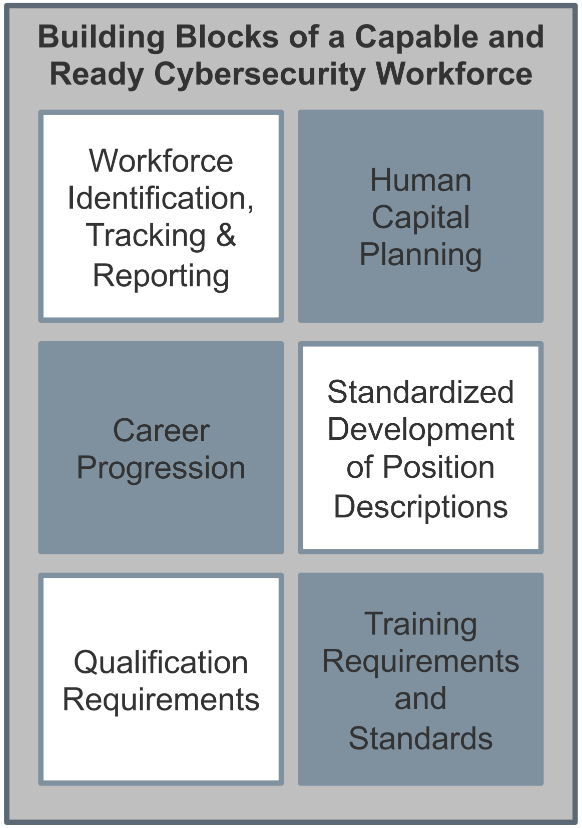
Use the NICE Cybersecurity Workforce Framework (NCWF) to build a strong cybersecurity workforce

Leverage the NCWF to establish the building blocks of a capable and ready cybersecurity workforce to effectively identify, recruit, develop and maintain cybersecurity talent.

The NCWF is a reference resource that offers:

1. A common and consistent **lexicon** that can be used by educators, employers, and employees.
2. **Criticality analysis** to identify knowledge, skills, abilities (KSAs), and tasks of in-demand cybersecurity work roles.
3. **Proficiency analysis** to understand the level of expertise required of a work role.

The blueprint will focus on the components in white squares.



Building Blocks of a Capable and Ready Cybersecurity Workforce

Workforce Identification, Tracking & Reporting	Human Capital Planning
Career Progression	Standardized Development of Position Descriptions
Qualification Requirements	Training Requirements and Standards

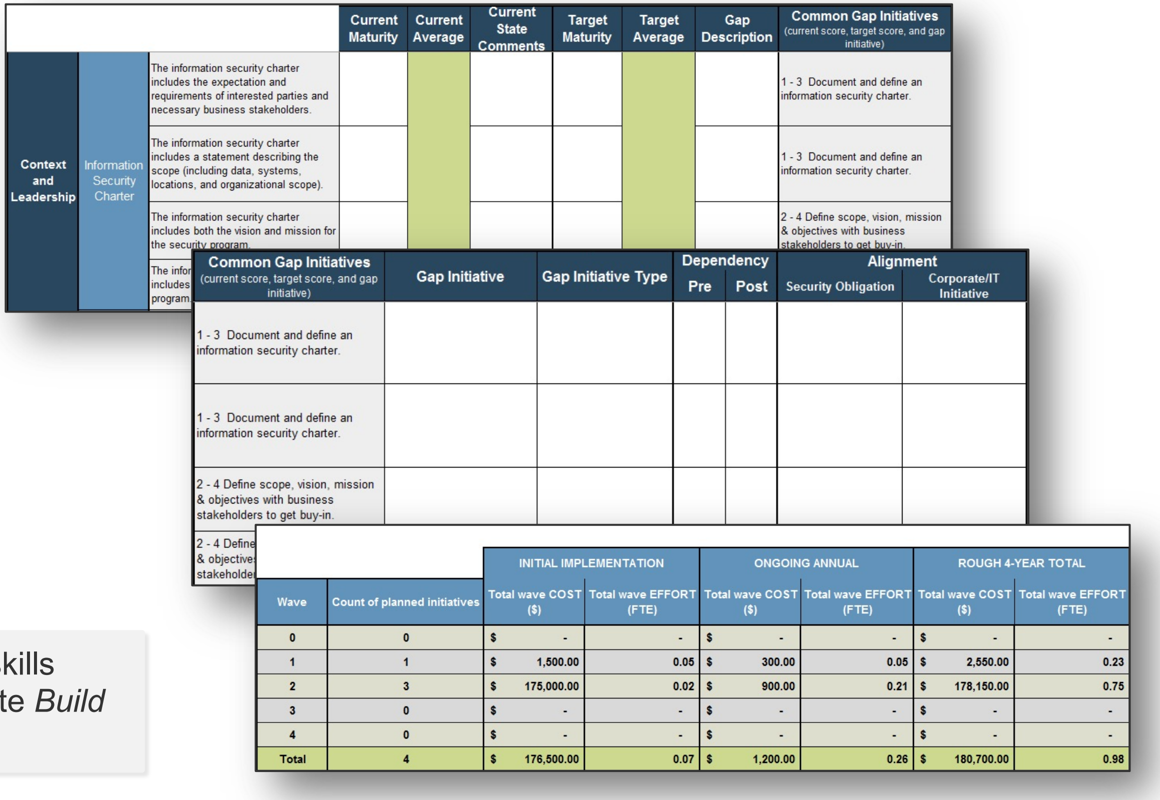
Adapted from NIST SP 800-181

For optimal results, consider Info-Tech's security strategy blueprint

Leverage Info-Tech's *Build an Information Security Strategy*

Improve your enterprise's security posture by integrating your security strategy with your cybersecurity sourcing plan.

The *Build an Information Security Strategy* blueprint will help you develop a strategy and roadmap to achieve your organization's security target state. Aligning with several best-practice frameworks (e.g. ISO 27000 series, CIS, COBIT 5, NIST SP800-53), Info-Tech's approach will help you understand your company's current vulnerabilities and obligations to identify, prioritize, and budget your initiatives.



			Current Maturity	Current Average	Current State Comments	Target Maturity	Target Average	Gap Description	Common Gap Initiatives (current score, target score, and gap initiative)
Context and Leadership	Information Security Charter	The information security charter includes the expectation and requirements of interested parties and necessary business stakeholders.							1 - 3 Document and define an information security charter.
		The information security charter includes a statement describing the scope (including data, systems, locations, and organizational scope).							1 - 3 Document and define an information security charter.
		The information security charter includes both the vision and mission for the security program.							2 - 4 Define scope, vision, mission & objectives with business stakeholders to get buy-in.
		The infor includes program.							

Common Gap Initiatives (current score, target score, and gap initiative)	Gap Initiative	Gap Initiative Type	Dependency		Alignment	
			Pre	Post	Security Obligation	Corporate/IT Initiative
1 - 3 Document and define an information security charter.						
1 - 3 Document and define an information security charter.						
2 - 4 Define scope, vision, mission & objectives with business stakeholders to get buy-in.						
2 - 4 Define & objective stakeholde						

		INITIAL IMPLEMENTATION		ONGOING ANNUAL		ROUGH 4-YEAR TOTAL	
Wave	Count of planned initiatives	Total wave COST ($)	Total wave EFFORT (FTE)	Total wave COST ($)	Total wave EFFORT (FTE)	Total wave COST ($)	Total wave EFFORT (FTE)
0	0	$ -	-	$ -	-	$ -	-
1	1	$ 1,500.00	0.05	$ 300.00	0.05	$ 2,550.00	0.23
2	3	$ 175,000.00	0.02	$ 900.00	0.21	$ 178,150.00	0.75
3	0	$ -	-	$ -	-	$ -	-
4	0	$ -	-	$ -	-	$ -	-
Total	4	$ 176,500.00	0.07	$ 1,200.00	0.26	$ 180,700.00	0.98

Info-Tech **Best Practice**

Have a security roadmap? Continue with this skills deck. Don't have a security roadmap? Complete *Build an Information Security Strategy* first.

Measured value for Guided Implementations

Engaging in GIs doesn't just offer valuable project advice, it also results in significant cost savings. Work smarter, not harder.

GI	Purpose	Measured Value
Identify Skill Needs for Target State	Determine the skill needs of your security initiatives.	Begin by identifying the skill needs of your desired future state. Get value by leveraging Info-Tech's templates and guidance. ***Example*** • Time Saved: 2 FTEs * 2 days * $80,000/year = ~$**1300**
Identify Technical Skill Gaps	Align skill needs of your security initiatives with current and/or future job role requirements.	Define job role requirements in current and future work roles and conduct a qualitative skills assessment on your current workforce. ***Example*** • Time Saved: 2 FTEs * 2 days * $80,000/year = ~$**1300**
Develop a Skills Sourcing Plan for Future Work Roles	Create a plan on how to address the skills gaps.	Identify the preferred way to acquire needed skills given key factors. ***Example*** • Time Saved: 2 FTEs * 5 days * $80,000/year = ~**$3,200**

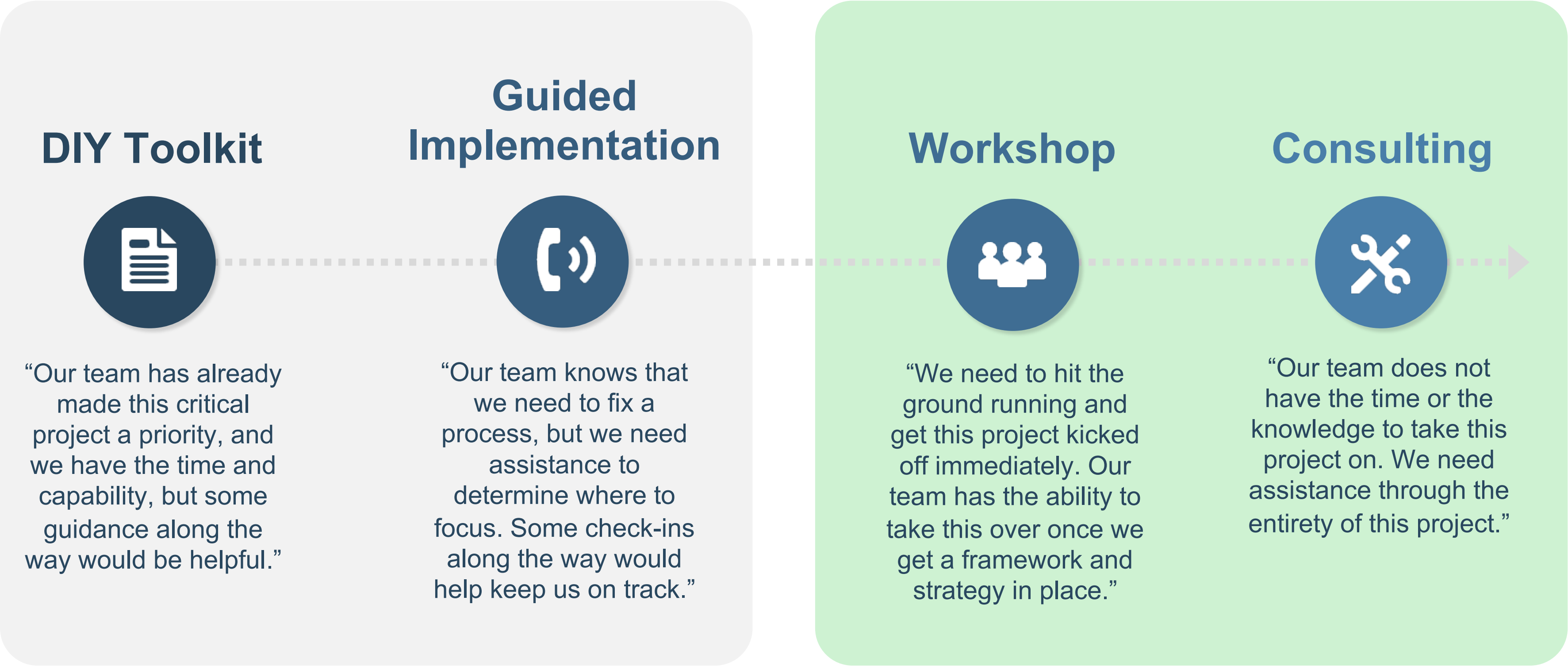
Use these icons to help direct you as you navigate this research

Use these icons to help guide you through each step of the blueprint and direct you to content related to the recommended activities.

This icon denotes a slide where a supporting Info-Tech tool or template will help you perform the activity or step associated with the slide. Refer to the supporting tool or template to get the best results and proceed to the next step of the project.

This icon denotes a slide with an associated activity. The activity can be performed either as part of your project or with the support of Info-Tech team members, who will come onsite to facilitate a workshop for your organization.

Info-Tech offers various levels of support to best suit your needs



DIY Toolkit

"Our team has already made this critical project a priority, and we have the time and capability, but some guidance along the way would be helpful."

Guided Implementation

"Our team knows that we need to fix a process, but we need assistance to determine where to focus. Some check-ins along the way would help keep us on track."

Workshop

"We need to hit the ground running and get this project kicked off immediately. Our team has the ability to take this over once we get a framework and strategy in place."

Consulting

"Our team does not have the time or the knowledge to take this project on. We need assistance through the entirety of this project."

Diagnostics and consistent frameworks used throughout all four options

Close the InfoSec Skills Gap: Develop a Technical Skills Sourcing Plan – project overview

	1. Identify Skill Needs for Target State	2. Identify Technical Skill Gaps	3. Develop a Skills Sourcing Plan for Future Work Roles
Best-Practice Toolkit	**1.1 Understand the Importance of Aligning Security Initiatives Skill Needs to Workforce Requirements** **1.2 Identify Needed Skills for Future Initiatives** **1.3 Document the Whiteboard Exercise** **1.4 Prioritize the Initiative Skill Gaps** **1.5 Adapt Current and Future Roles to the Needs of Your Future Environment**	**2.1 Brainstorm the Technical Skills Needed for Your Organization's Current and Future Work Roles** **2.2 Leverage Info-tech's Job Description Templates to Determine the Skills Required for Your Work Roles** **2.3 Use the NICE Cybersecurity Workforce Framework (NCWF) as a Guide to Establishing Skill Expectations** **2.4 Document the Technical Skills of Your *Current* Workforce Roles and Identify Employee Skill Gaps** **2.5 Document Technical Skills Required for *Future* Work Roles**	**3.1 Review the Five Key Factors for Skills Acquisition** **3.2 Explore Your Options for Sourcing Skills** **3.3 Determine How to Acquire Needed Skills** **3.4 Review Decision**
Guided Implementations	☎ Define security roadmap skill needs. ☎ Prioritize and associate roles with the initiative skill gaps.	☎ Align role requirements with future initiative skill needs.	☎ Understand and define the factors that influence the skills sourcing plan, and discuss options for sourcing skills. ☎ Score key factors against needed skill, and determine how to source a skill.
Onsite Workshop	**Module 1:** Identify Skill Needs for Target State	**Module 2:** Identify Technical Skill Gaps	**Module 3:** Develop a Skills Sourcing Plan
	Phase 1 Outcome: • Identify skills needed to support the organization's security initiatives. • Identify and define current and future roles that align with security initiatives.	**Phase 2 Outcome:** • Identify and define skill requirements of current and future roles that align with security initiatives.	**Phase 3 Outcome:** • Create impact scoring scales that reflect current business context and upcoming security initiatives for the five key factors that influence your decision to build or buy needed skills. • Decide how to acquire skills.

Workshop overview

Contact your account representative or email Workshops@InfoTech.com for more information.

	Workshop Day 1	Workshop Day 2	Workshop Day 3	Workshop Day 4
Activities	**Identify Skill Needs for Target State** **1.1** Understand the importance of aligning security initiatives skill needs to workforce requirements. **1.2** Identify needed skills for future initiatives. **1.3** Prioritize the initiative skill gaps.	**Define Technical Skill Requirements** **2.1** Assign work roles to the needs of your future environment. **2.2** Discuss the NICE Cybersecurity Workforce Framework. **2.3** Develop technical skill requirements for current and future work roles. .	**Acquire Technical skills** **3.1** Continue developing technical skill requirements for current and future work roles. **3.2** Conduct *Current Workforce Skills Assessment.* **3.3** Discuss methods of acquiring skills. **3.4** Develop a plan to acquire skills.	**Plan to Execute Action Plan** **4.1** Review skills acquisition plan. **4.2** Discuss training and certification opportunities for staff. **4.3** Discuss next steps for closing the skills gap. **4.4** Debrief.
Deliverables	*1. Security Initiative Skills Guide* *2. Skills Gap Prioritization Tool*	*1. Skills Gap Prioritization Tool* *2. Technical Skills Workbook* *3. Current Workforce Skills Assessment*	*1. Technical Skills Workbook* *2. Current Workforce Skills Assessment*	*1. Technical Skills Workbook*

PHASE 1

Identify Skill Needs for Target State

Close the InfoSec Skills Gap: Develop a Technical Skills Sourcing Plan

Phase 1 outline

☎ **Call 1-888-670-8889** or email GuidedImplementations@InfoTech.com for more information.

Complete these steps on your own, or call us to complete a guided implementation. A guided implementation is a series of 2-3 advisory calls that help you execute each phase of a project. They are included in most advisory memberships.

Guided Implementation 1: Identify Skill Needs for Target State

Proposed Time to Completion: 3 weeks

Steps 1.1-1.3: Define Security Roadmap Skill Needs

Start with an analyst kick-off call:

- Identify skills needed to support the organization's security initiatives.

Then complete these activities…

- Review your organization's security roadmap for a list of initiatives. Identify skills required to successfully execute the initiative.

With these tools & templates:

Security Initiative Skills Guide

Steps 1.4-1.5: Prioritize and Associate Roles With the Initiative Skill Gaps

Review findings with analyst:

- Review future initiatives skill needs.

Then complete these activities…

- Prioritize security initiative skill needs.
- Identify current and future roles that align to the organization's future skill needs.
- Associate work roles with skill needs.

With these tools & templates:

Skills Gap Prioritization Tool

Phase 1 Results & Insights:

- Identify skills needed in the organization to support security initiatives.
- Create a *Security Initiative Skills Guide* that captures future skill needs.
- Prioritize and assign roles to the organization's future skill needs.

1.1 Understand the importance of aligning security initiatives skill needs to workforce requirements

- Mapping the skill needs of your security initiatives to your work roles provides the **link between your workforce and cybersecurity strategy.**
- To successfully execute the initiatives of your security strategy, your enterprise **must have or obtain the necessary skills.** Otherwise, the initiatives cannot be carried out to their full potential.
- IT operations are often involved in performing some security tasks for the enterprise. Defining cybersecurity role requirements with related security initiatives means you can better **separate the responsibilities of security professionals and those of IT operations.** As a result, organizations can gain awareness of where gaps in skills and communication exist.

> “*No enterprise can be secure without the right people, in the right place, with the right skills and empowered with the right authorities and supporting resources.*”
>
> – Cybersecurity Workforce Handbook, 2014

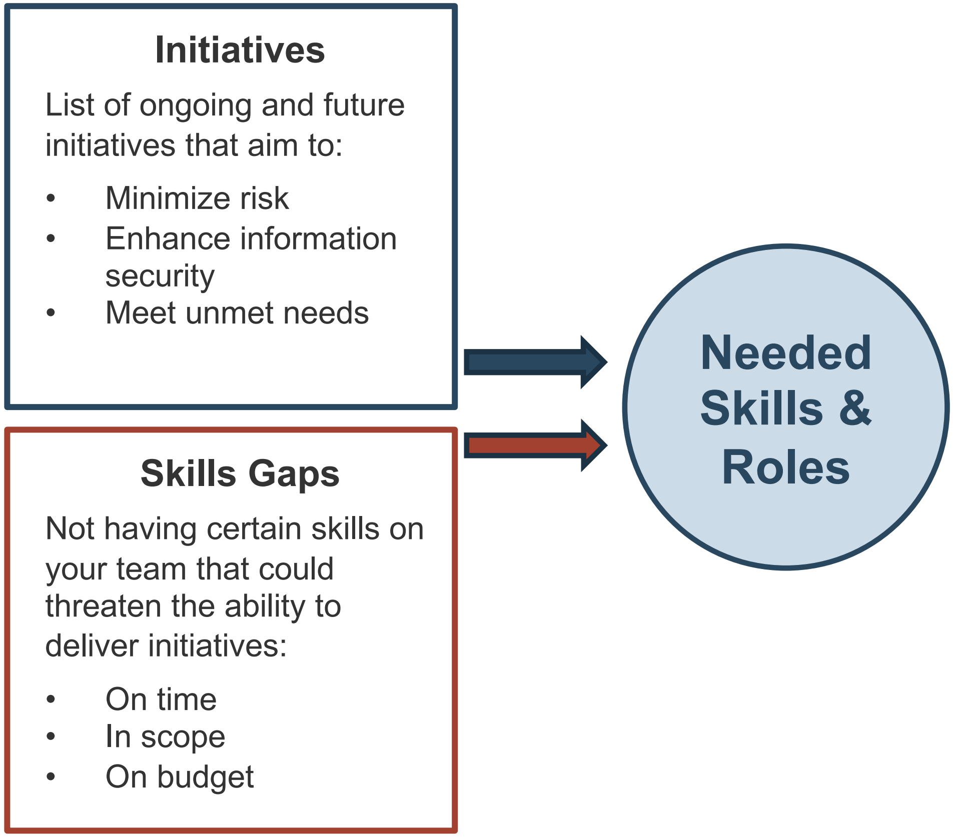
1.2 Identify needed skills for future initiatives

1.2(a) Whiteboard Exercise

1. **Identify the timeline of the security roadmap.**

2. **List and describe initiatives.**

3. **Identify which skills are lacking in your workforce that are required to execute the initiatives.**



Initiatives

List of ongoing and future initiatives that aim to:

- Minimize risk
- Enhance information security
- Meet unmet needs

Skills Gaps

Not having certain skills on your team that could threaten the ability to deliver initiatives:

- On time
- In scope
- On budget

Needed Skills & Roles

Materials

- Whiteboard
- *Security Initiative Skills Guide*

Participants

- Security management
- Key project stakeholders

OUTPUTS

- Skills needed to support initiatives and mitigate risks

Info-Tech **Insight**

Prepare for the long term. Looking only as far as the needs of the next project will lead to a constant skills shortage with no plan to address it. Prevent this from happening by using your security strategy as a guide to predict the skills your organization will require in the future.

1.2 Define and describe impact of skills gap

1.2(b) Whiteboard Exercise

4 **Define impact rating scale.**

Consider using the variables below to define your impact levels:

- Timeline delays
- Efficiency impact (increased processing time)
- Scope of availability issue (number of systems or users)
- Critical function degradation/loss
- Business damages (loss of productivity, financial penalties, etc.)

Low	Medium	High
• Negligible functional impact to the organization. • Timeline delay: Successful execution of the initiative will be delayed no longer than a month.	• Substantial functional impact to the organization. • Timeline delay: Carrying out the initiative will be delayed by up to six months.	• The skills gap will threaten the successful execution of the initiative. • Timeline delay: The initiative will be delayed by more than six months.

5 **Describe the impact of the skills gap to the organization.**

1.2

Define and assign likelihood of skills gap influencing security initiative

1.2(c) Whiteboard Exercise

6 **Describe and assign the likelihood of the skills gap having an influence on the execution of the initiative.**

- **High:** The skills gap will likely hinder the execution of the initiative.
- **Medium:** The skills gap may possibly impede the execution of the initiative.
- **Low:** The skills gap is unlikely to have an influence on the deployment of the initiative.

7 **Add additional comments or notes concerning the skills gap.**

- Is the affected initiative a priority?
- What is the initiative’s timeline? When is it to be deployed?
- Has your organization discussed how they intend to resource the skills associated with the initiative (e.g. hire, outsource, contract, train)?
- What additional factors need to be considered in carrying out the initiative as it relates to the skills gap (e.g. workforce supply, budget, current technology)?

1.2 Example of a security initiative with a skills gap

1.2(d) Whiteboard Exercise

Initiative from security roadmap: Develop a data classification program.

Skills gap associated with a data classification program:

Skills Gap	Impact	Likelihood of Skills Gap Influencing Initiative (H/M/L)
The organization has limited knowledge of what and where data exists in the organization.	**Medium** • Data discovery is a time-consuming process and often the bottleneck of carrying out a data classification program.	**Low** • Senior management has emphasized that data discovery must be prioritized this year.
There is a lack of expertise in data regulations within the organization.	**High** • Data classification policy and standard must reflect privacy regulations (e.g. PCI-DSS, GDPR, PII, HIPAA). • A comprehensive policy and standard cannot be developed without knowledge in data privacy.	**Medium** • Expertise can be outsourced.

Info-Tech **Best Practice**

Carry out this exercise for all initiatives on your security roadmap. Start with high-priority initiatives and then move to less urgent items.

1.3 Document the whiteboard exercise

1.3 Security Initiative Skills Guide

Overview

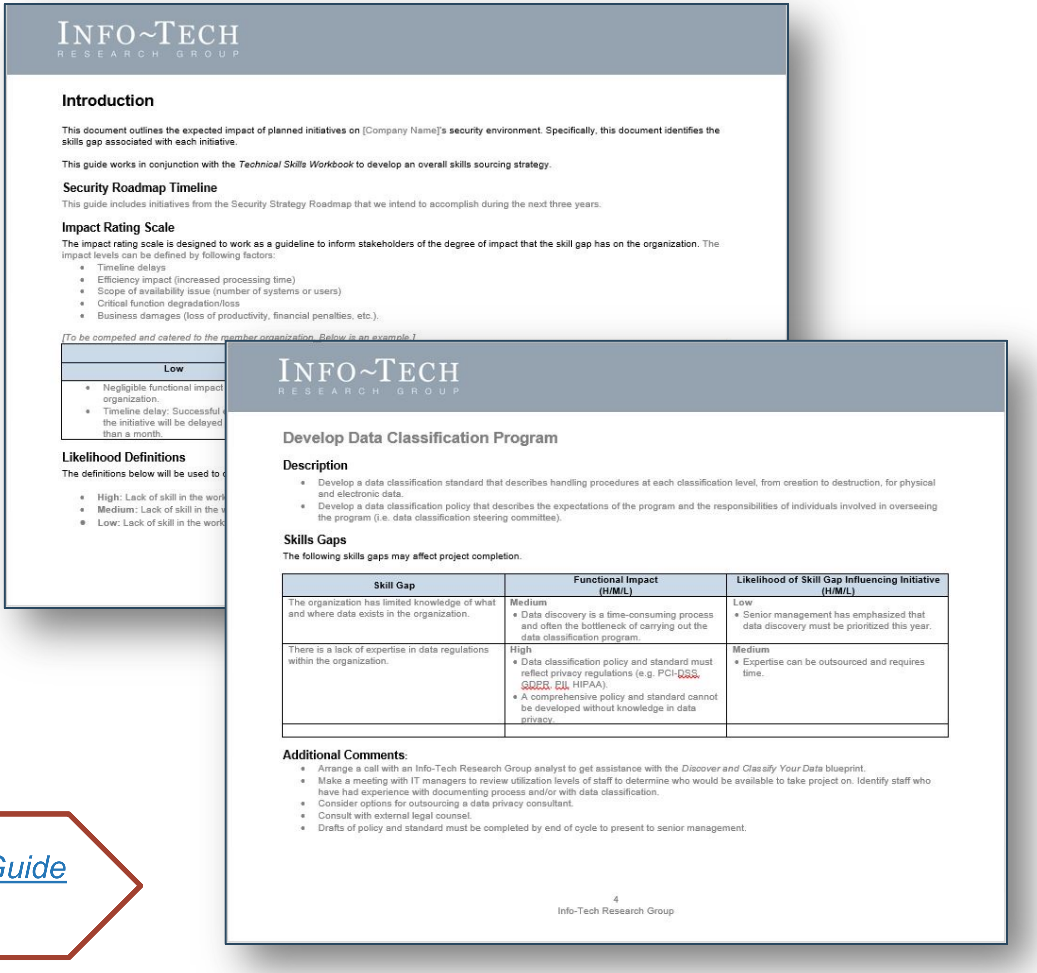
The *Security Initiative Skills Guide* aims to document needed skills for each security initiative.

Instructions

Customize the document to reflect your organization by replacing or removing the grey text in the document.

Define:

- Timeline of security roadmap
- Impact rating scale
- Likelihood definitions
- Security initiatives
- Skills gap



INFO~TECH
RESEARCH GROUP

Introduction

This document outlines the expected impact of planned initiatives on [Company Name]'s security environment. Specifically, this document identifies the skills gap associated with each initiative.

This guide works in conjunction with the *Technical Skills Workbook* to develop an overall skills sourcing strategy.

Security Roadmap Timeline

This guide includes initiatives from the Security Strategy Roadmap that we intend to accomplish during the next three years.

Impact Rating Scale

The impact rating scale is designed to work as a guideline to inform stakeholders of the degree of impact that the skill gap has on the organization. The impact levels can be defined by following factors:

- Timeline delays
- Efficiency impact (increased processing time)
- Scope of availability issue (number of systems or users)
- Critical function degradation/loss
- Business damages (loss of productivity, financial penalties, etc.).

[To be competed and catered to the member organization. Below is an example.]

Low
• Negligible functional impact organization. • Timeline delay: Successful the initiative will be delayed than a month.

Likelihood Definitions

The definitions below will be used to

- **High**: Lack of skill in the work
- **Medium**: Lack of skill in the w
- **Low**: Lack of skill in the work

INFO~TECH
RESEARCH GROUP

Develop Data Classification Program

Description

- Develop a data classification standard that describes handling procedures at each classification level, from creation to destruction, for physical and electronic data.
- Develop a data classification policy that describes the expectations of the program and the responsibilities of individuals involved in overseeing the program (i.e. data classification steering committee).

Skills Gaps

The following skills gaps may affect project completion.

Skill Gap	Functional Impact (H/M/L)	Likelihood of Skill Gap Influencing Initiative (H/M/L)
The organization has limited knowledge of what and where data exists in the organization.	**Medium** • Data discovery is a time-consuming process and often the bottleneck of carrying out the data classification program.	**Low** • Senior management has emphasized that data discovery must be prioritized this year.
There is a lack of expertise in data regulations within the organization.	**High** • Data classification policy and standard must reflect privacy regulations (e.g. PCI-DSS, GDPR, PII, HIPAA). • A comprehensive policy and standard cannot be developed without knowledge in data privacy.	**Medium** • Expertise can be outsourced and requires time.

Additional Comments:

- Arrange a call with an Info-Tech Research Group analyst to get assistance with the *Discover and Classify Your Data* blueprint.
- Make a meeting with IT managers to review utilization levels of staff to determine who would be available to take project on. Identify staff who have had experience with documenting process and/or with data classification.
- Consider options for outsourcing a data privacy consultant.
- Consult with external legal counsel.
- Drafts of policy and standard must be completed by end of cycle to present to senior management.

4
Info-Tech Research Group

Use Info-Tech's *Security Initiative Skills Guide* template.

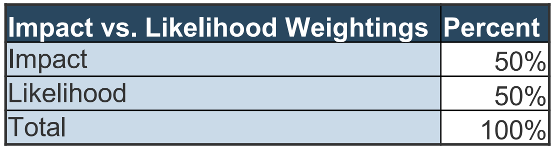
1.4 Prioritize the initiative skill gaps in the *Skills Gap Prioritization Tool*

1.4 Skills Gap Prioritization Tool

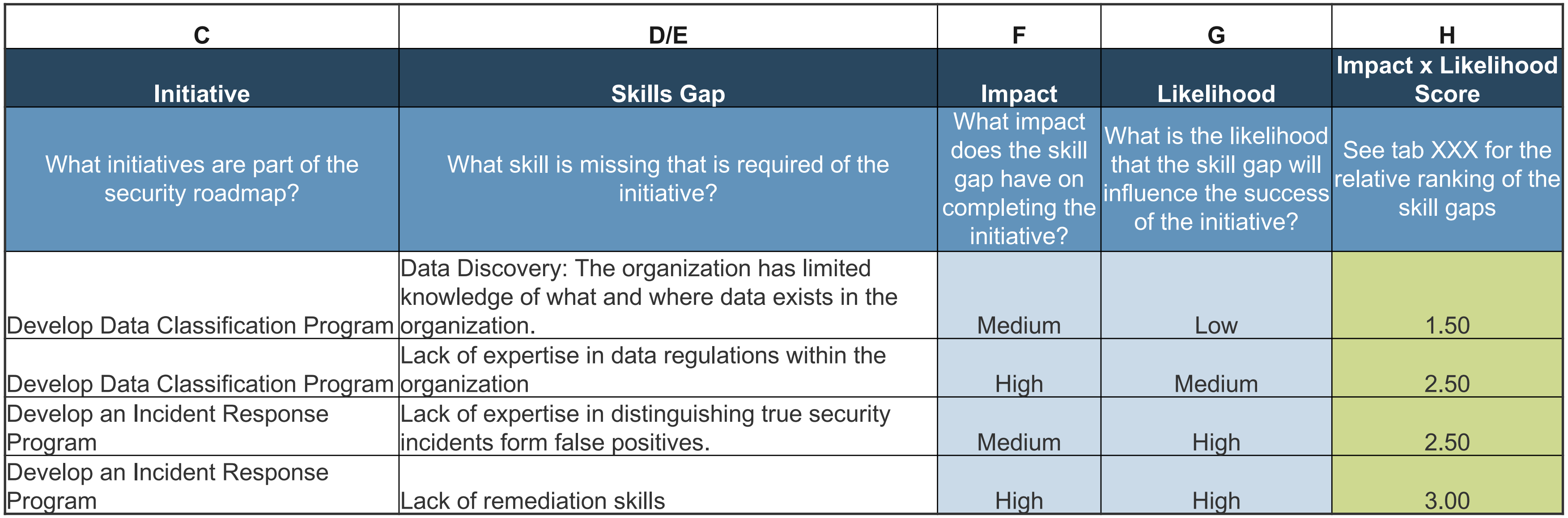
Transfer data from the *Security Initiative Skills Guide* into the *Skills Gap Prioritization Tool*.

Tab 2. Data Entry

1. Adjust impact and likelihood weightings in Table 1.
2. Input impact and likelihood definitions into Table 2 and Table 3.
3. Input initiatives, skills gap, impact score, and likelihood scores into Table 4. The impact x likelihood score will auto populate in Column H.



Impact vs. Likelihood Weightings	Percent
Impact	50%
Likelihood	50%
Total	100%



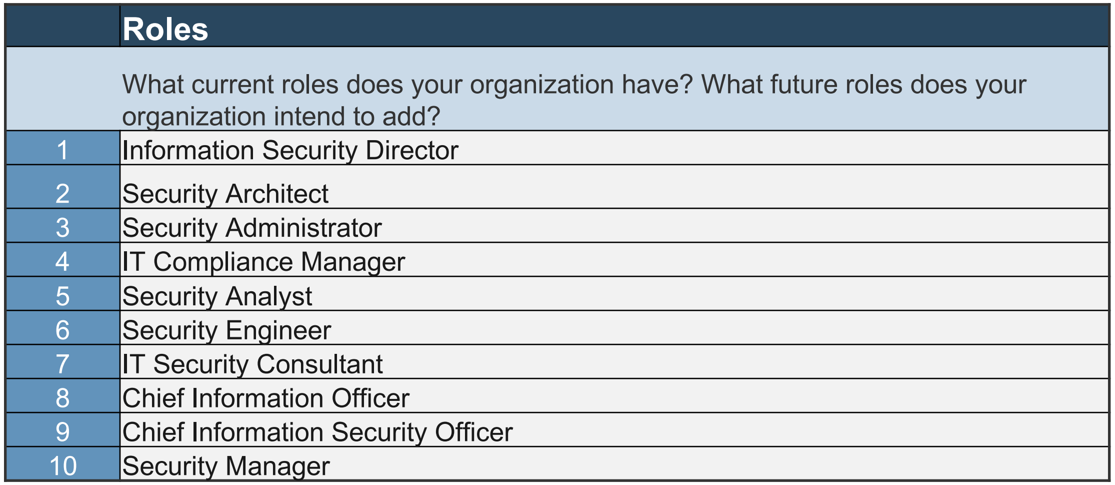
C	D/E	F	G	H
Initiative	**Skills Gap**	**Impact**	**Likelihood**	**Impact x Likelihood Score**
What initiatives are part of the security roadmap?	What skill is missing that is required of the initiative?	What impact does the skill gap have on completing the initiative?	What is the likelihood that the skill gap will influence the success of the initiative?	See tab XXX for the relative ranking of the skill gaps
Develop Data Classification Program	Data Discovery: The organization has limited knowledge of what and where data exists in the organization.	Medium	Low	1.50
Develop Data Classification Program	Lack of expertise in data regulations within the organization	High	Medium	2.50
Develop an Incident Response Program	Lack of expertise in distinguishing true security incidents form false positives.	Medium	High	2.50
Develop an Incident Response Program	Lack of remediation skills	High	High	3.00

1.5 Adapt current and future roles to the needs of your future environment

1.5 Skills Gap Prioritization Tool

Tab 3. Results

4 Input cybersecurity roles that your organization currently has and new cybersecurity roles that your organization may need or intend to have in the future in Table 5.



	Roles
	What current roles does your organization have? What future roles does your organization intend to add?
1	Information Security Director
2	Security Architect
3	Security Administrator
4	IT Compliance Manager
5	Security Analyst
6	Security Engineer
7	IT Security Consultant
8	Chief Information Officer
9	Chief Information Security Officer
10	Security Manager

5 Table 6 ranks the skill gap's impact x likelihood score. In Columns F through H, input the role that is responsible for obtaining the skill gap.

Tab 4. Role Skills Tables

6 Based on Table 6, Tab 4 will auto-group ranked skill gaps by work role.

PHASE 2

Identify Technical Skill Gaps

Close the InfoSec Skills Gap: Develop a Technical Skills Sourcing Plan

Info-Tech Research Group, Inc. is a global leader in providing IT research and advice.
Info-Tech's products and services combine actionable insight and relevant advice with
ready-to-use tools and templates that cover the full spectrum of IT concerns.

Phase 2 outline

☎ **Call 1-888-670-8889** or email GuidedImplementations@InfoTech.com for more information.

Complete these steps on your own, or call us to complete a guided implementation. A guided implementation is a series of 2-3 advisory calls that help you execute each phase of a project. They are included in most advisory memberships.

Guided Implementation 2: Identify Technical Skill Gaps

Proposed Time to Completion: 3 weeks

Steps 2.1-2.5: Identify Technical Skill Gaps

Start with an analyst kick-off call:

- Align role requirements with future security initiative skill needs.

Then complete these activities…

- Brainstorm the technical skills needed for your organization's current and future work roles.
- Review the NICE Cybersecurity Workforce Framework (NCWF) and previous organizational job descriptions as a guide to establishing skill expectations.
- Conduct a qualitative technical skills assessment on your current workforce.

With these tools & templates:

Current Workforce Skills Assessment

Technical Skills Workbook, Tab 1

Phase 2 Results & Insights:

- Define skill sets for current and future roles that are reflective of your organization's future initiatives skill needs.

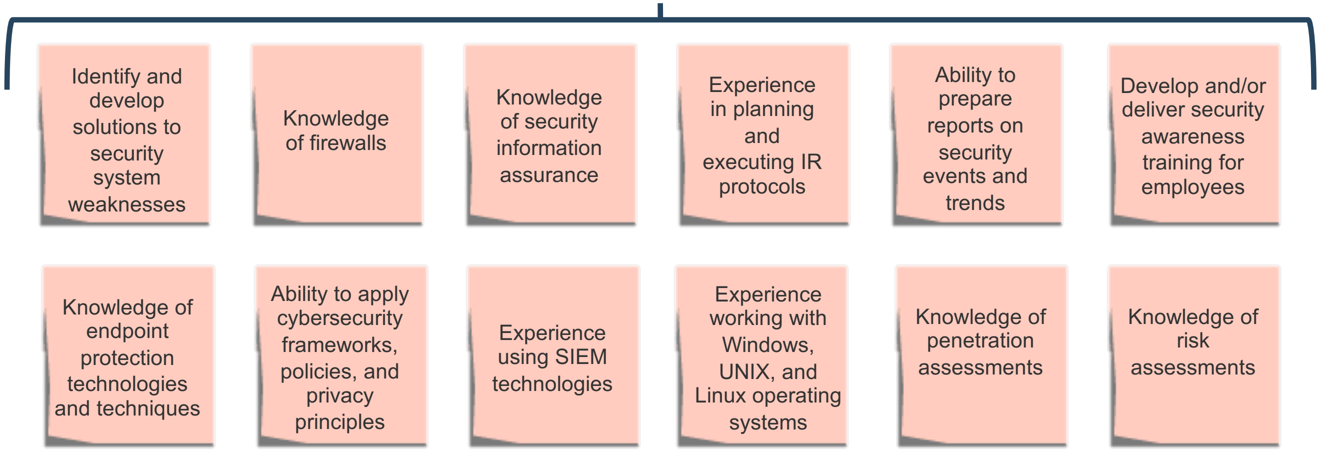
2.1 Brainstorm the technical skills needed for your organization's current and future work roles

2.1 Whiteboard Exercise

Use the following resources:

- Tab 4 in the *Skills Gap Prioritization Tool*.
- Job descriptions used by your organization's human resources office.
- The National Initiative Cybersecurity Education (NICE) Workforce Framework.

Security Analyst



- Identify and develop solutions to security system weaknesses
- Knowledge of firewalls
- Knowledge of security information assurance
- Experience in planning and executing IR protocols
- Ability to prepare reports on security events and trends
- Develop and/or deliver security awareness training for employees
- Knowledge of endpoint protection technologies and techniques
- Ability to apply cybersecurity frameworks, policies, and privacy principles
- Experience using SIEM technologies
- Experience working with Windows, UNIX, and Linux operating systems
- Knowledge of penetration assessments
- Knowledge of risk assessments

› Transfer the list of skills for security-related work roles currently held by employees into the *Current Workforce Skills Assessment* tool.

› For future work roles, transfer their skillsets into the *Technical Skills Workbook*.

Materials

- Whiteboard
- *Skills Gap Prioritization Tool*

Participants

- Security management
- Key project stakeholders

OUTPUTS

- List of skills required by work role that reflects the security roadmap

2.2 Leverage Info-Tech's job description templates to determine the skills required for your work roles

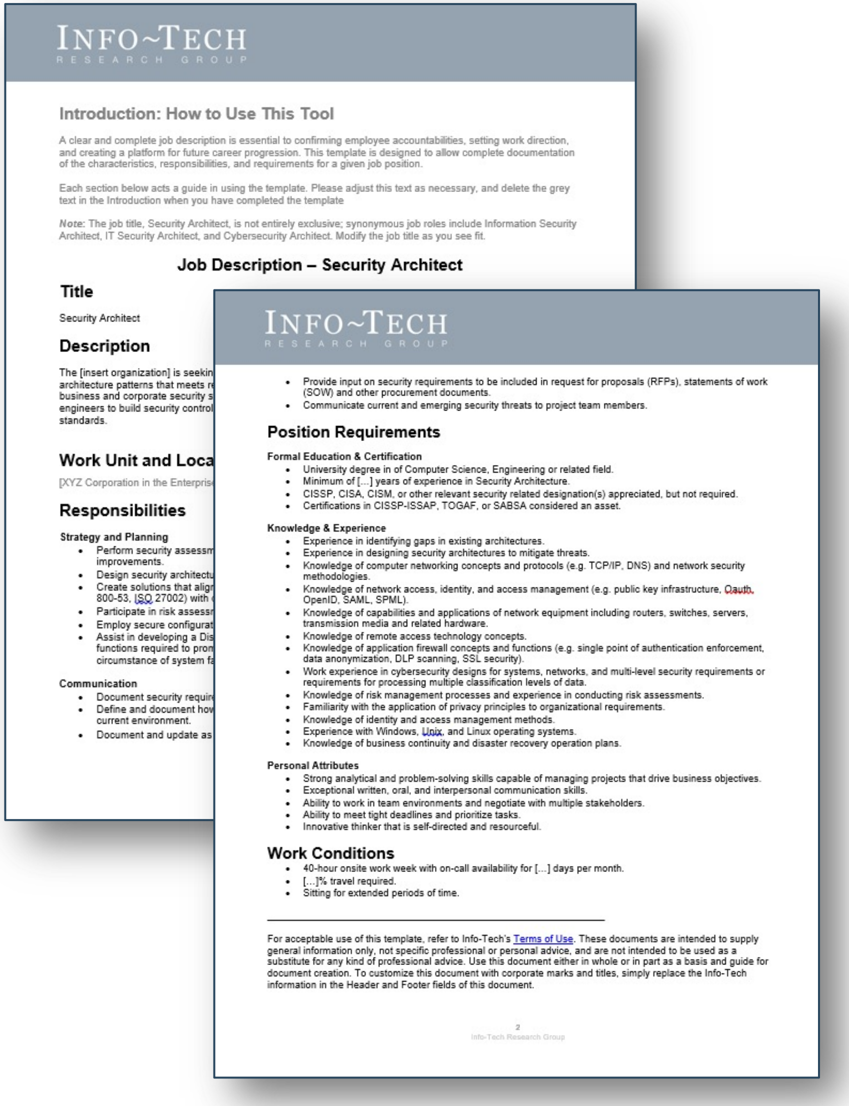
Extract technical skills from Info-Tech's repository of job descriptions to identify skills gaps.

Roles included in this blueprint:

- *Security Architect*
- *Information Security Compliance Manager*
- *Chief Information Security Officer*
- *IT Security Analyst*
- *Security Administrator*

Job descriptions include editable sections:

- Responsibilities
- Position Requirements
  - Formal Education & Certification
  - Knowledge & Experience
  - Personal Attributes
- Work Conditions



INFO~TECH
RESEARCH GROUP

Introduction: How to Use This Tool

A clear and complete job description is essential to confirming employee accountabilities, setting work direction, and creating a platform for future career progression. This template is designed to allow complete documentation of the characteristics, responsibilities, and requirements for a given job position.

Each section below acts a guide in using the template. Please adjust this text as necessary, and delete the grey text in the Introduction when you have completed the template

Note: The job title, Security Architect, is not entirely exclusive; synonymous job roles include Information Security Architect, IT Security Architect, and Cybersecurity Architect. Modify the job title as you see fit.

Job Description – Security Architect

Title

Security Architect

Description

The [insert organization] is seekin
architecture patterns that meets re
business and corporate security s
engineers to build security control
standards.

Work Unit and Loca

[XYZ Corporation in the Enterprise

Responsibilities

Strategy and Planning
- Perform security assessm
  improvements.
- Design security architectu
- Create solutions that align
  800-53, ISO 27002) with
- Participate in risk assessm
- Employ secure configurat
- Assist in developing a Dis
  functions required to prom
  circumstance of system fa

Communication
- Document security require
- Define and document how
  current environment.
- Document and update as

INFO~TECH
RESEARCH GROUP

- Provide input on security requirements to be included in request for proposals (RFPs), statements of work (SOW) and other procurement documents.
- Communicate current and emerging security threats to project team members.

Position Requirements

Formal Education & Certification
- University degree in of Computer Science, Engineering or related field.
- Minimum of [...] years of experience in Security Architecture.
- CISSP, CISA, CISM, or other relevant security related designation(s) appreciated, but not required.
- Certifications in CISSP-ISSAP, TOGAF, or SABSA considered an asset.

Knowledge & Experience
- Experience in identifying gaps in existing architectures.
- Experience in designing security architectures to mitigate threats.
- Knowledge of computer networking concepts and protocols (e.g. TCP/IP, DNS) and network security methodologies.
- Knowledge of network access, identity, and access management (e.g. public key infrastructure, Oauth, OpenID, SAML, SPML).
- Knowledge of capabilities and applications of network equipment including routers, switches, servers, transmission media and related hardware.
- Knowledge of remote access technology concepts.
- Knowledge of application firewall concepts and functions (e.g. single point of authentication enforcement, data anonymization, DLP scanning, SSL security).
- Work experience in cybersecurity designs for systems, networks, and multi-level security requirements or requirements for processing multiple classification levels of data.
- Knowledge of risk management processes and experience in conducting risk assessments.
- Familiarity with the application of privacy principles to organizational requirements.
- Knowledge of identity and access management methods.
- Experience with Windows, Unix, and Linux operating systems.
- Knowledge of business continuity and disaster recovery operation plans.

Personal Attributes
- Strong analytical and problem-solving skills capable of managing projects that drive business objectives.
- Exceptional written, oral, and interpersonal communication skills.
- Ability to work in team environments and negotiate with multiple stakeholders.
- Ability to meet tight deadlines and prioritize tasks.
- Innovative thinker that is self-directed and resourceful.

Work Conditions
- 40-hour onsite work week with on-call availability for [...] days per month.
- [...]% travel required.
- Sitting for extended periods of time.

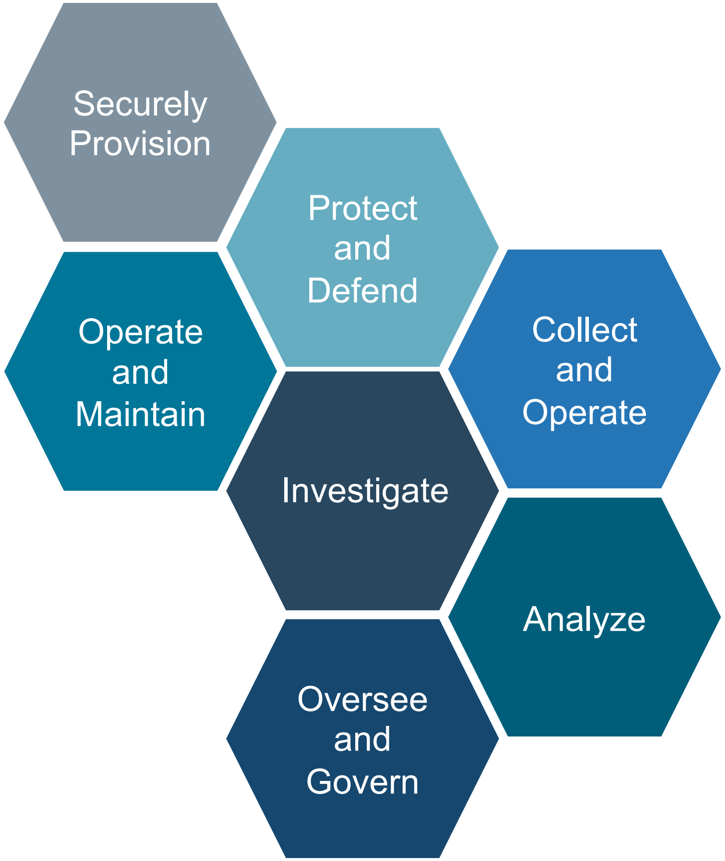
For acceptable use of this template, refer to Info-Tech's Terms of Use. These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.

2
Info-Tech Research Group

2.3 Use the NICE Cybersecurity Workforce Framework (NCWF) as a guide to establishing skill expectations

The NCWF is a workforce guideline that categorizes and describes the knowledge, skills, and abilities of more than 50 cybersecurity work roles. The NCWF:

- Provides organizations a common, consistent lexicon to help identify, recruit, develop, and retain cybersecurity talent.
- Establishes baseline skill standards, making it easier for organizations to identify skills gaps.
- Organizes cybersecurity job roles into seven categories (refer to the image on the right).



Info-Tech **Insight**

Adapt your roles and descriptions as best you can to the NCWF. The structure of security workforces and definitions of worker roles and their associated skill sets differ among companies, making it difficult to know how to develop a stronger workforce. Aligning your workforce to the NCWF can help clarify what skills your organization requires.

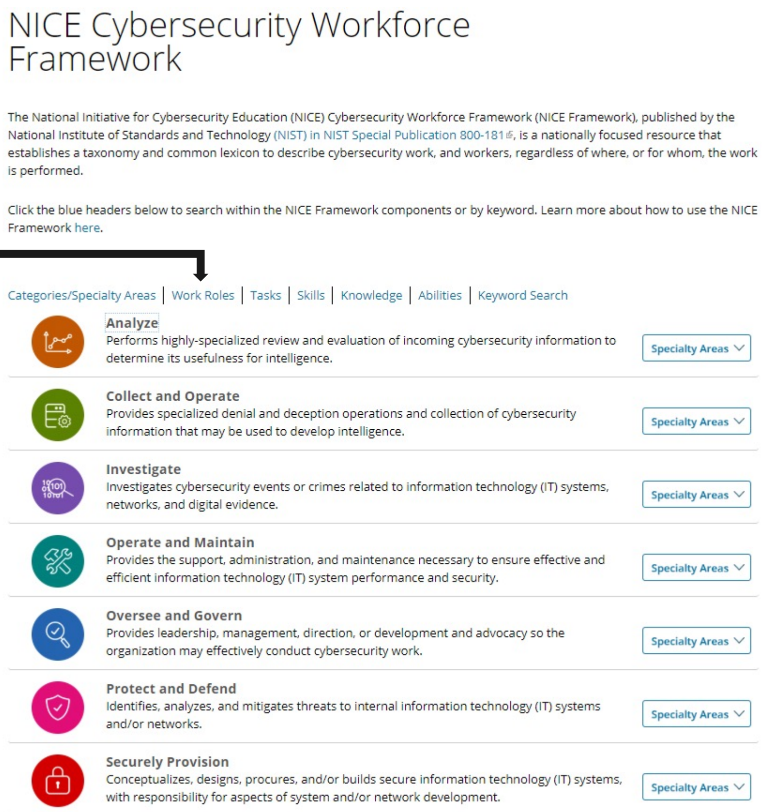
2.3

Use the NCWF as a guide for establishing skill expectations

NICCS™

Access a web friendly version of the NCWF on the National Initiative for Cybersecurity Careers and Studies (NICCS) website to quickly identify the knowledge, skills, and abilities (KSAs) and capability indicators of cybersecurity work roles.

1 Click on Work Roles



NICE Cybersecurity Workforce Framework

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), published by the National Institute of Standards and Technology (NIST) in NIST Special Publication 800-181, is a nationally focused resource that establishes a taxonomy and common lexicon to describe cybersecurity work, and workers, regardless of where, or for whom, the work is performed.

Click the blue headers below to search within the NICE Framework components or by keyword. Learn more about how to use the NICE Framework here.

Categories/Specialty Areas | Work Roles | Tasks | Skills | Knowledge | Abilities | Keyword Search

Analyze
Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Specialty Areas

Collect and Operate
Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Specialty Areas

Investigate
Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.
Specialty Areas

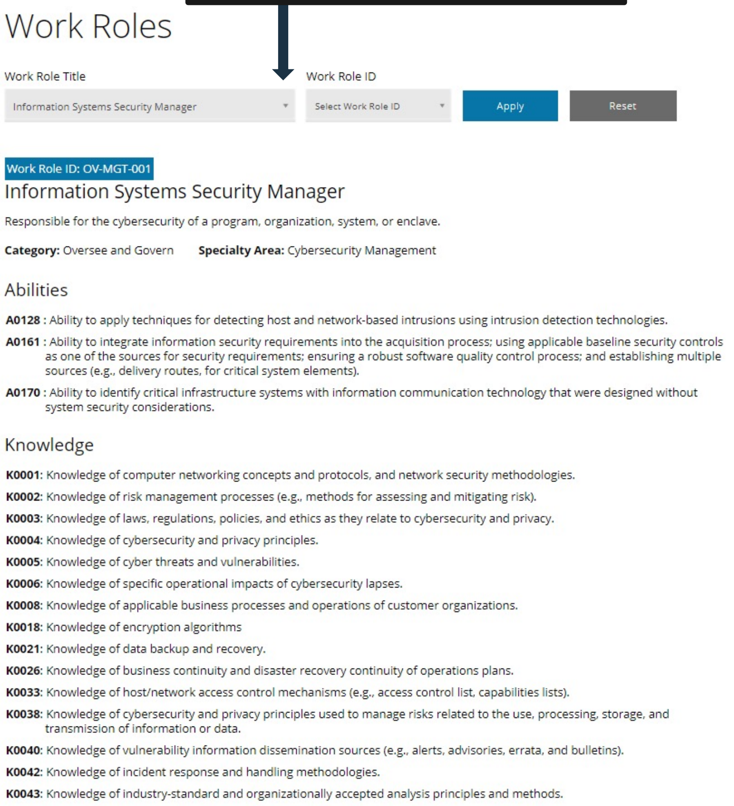
Operate and Maintain
Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Specialty Areas

Oversee and Govern
Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Specialty Areas

Protect and Defend
Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Specialty Areas

Securely Provision
Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Specialty Areas

2 Use the drop-down menu to select the Work Role Title



Work Roles

Work Role Title: Information Systems Security Manager
Work Role ID: Select Work Role ID
Apply
Reset

Work Role ID: OV-MGT-001

Information Systems Security Manager

Responsible for the cybersecurity of a program, organization, system, or enclave.

Category: Oversee and Govern **Specialty Area:** Cybersecurity Management

Abilities

A0128 : Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

A0161 : Ability to integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources (e.g., delivery routes, for critical system elements).

A0170 : Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.

Knowledge

K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.

K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.

K0004: Knowledge of cybersecurity and privacy principles.

K0005: Knowledge of cyber threats and vulnerabilities.

K0006: Knowledge of specific operational impacts of cybersecurity lapses.

K0008: Knowledge of applicable business processes and operations of customer organizations.

K0018: Knowledge of encryption algorithms

K0021: Knowledge of data backup and recovery.

K0026: Knowledge of business continuity and disaster recovery continuity of operations plans.

K0033: Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).

K0038: Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.

K0040: Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).

K0042: Knowledge of incident response and handling methodologies.

K0043: Knowledge of industry-standard and organizationally accepted analysis principles and methods.

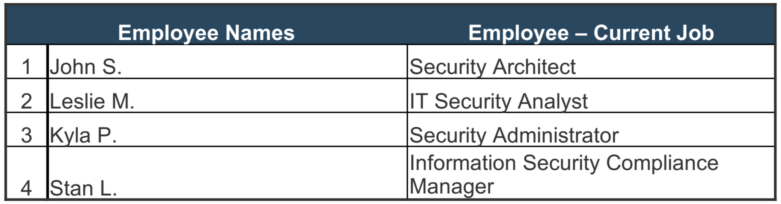
2.4

Document the technical skills of your *current* workforce roles and identify employee skill gaps

2.4 Current Workforce Skills Assessment

Tab 2. Workforce Inventory

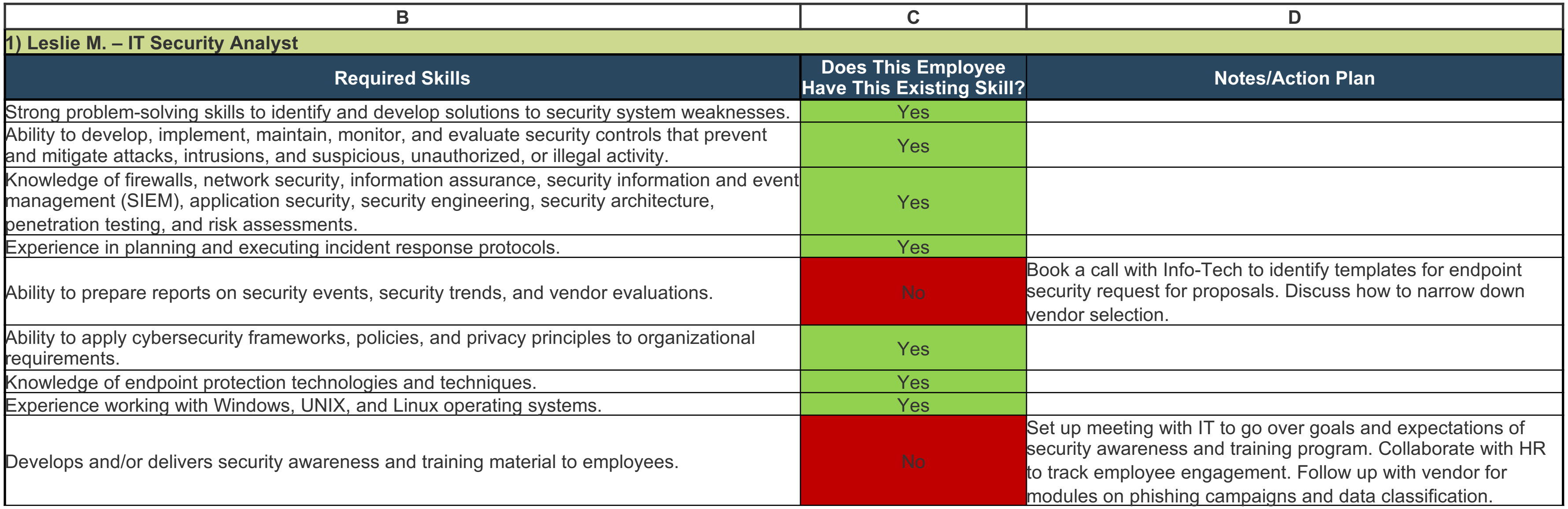
1 List all employees in your organization who contribute to IT security. Input data of employees who share the same roles consecutively.



	Employee Names	Employee – Current Job
1	John S.	Security Architect
2	Leslie M.	IT Security Analyst
3	Kyla P.	Security Administrator
4	Stan L.	Information Security Compliance Manager

Tab 3. Employee Scorecard

2 Referring to Exercise 2.1, transfer the list of skills relating to the employee's job role in Column B. For each skill, use the drop-down menu to inventory the employee's skill set. Use Column D to record any additional notes and/or an action plan for enhancing the corresponding skill.



B	C	D
1) Leslie M. – IT Security Analyst		
Required Skills	**Does This Employee Have This Existing Skill?**	**Notes/Action Plan**
Strong problem-solving skills to identify and develop solutions to security system weaknesses.	Yes	
Ability to develop, implement, maintain, monitor, and evaluate security controls that prevent and mitigate attacks, intrusions, and suspicious, unauthorized, or illegal activity.	Yes	
Knowledge of firewalls, network security, information assurance, security information and event management (SIEM), application security, security engineering, security architecture, penetration testing, and risk assessments.	Yes	
Experience in planning and executing incident response protocols.	Yes	
Ability to prepare reports on security events, security trends, and vendor evaluations.	No	Book a call with Info-Tech to identify templates for endpoint security request for proposals. Discuss how to narrow down vendor selection.
Ability to apply cybersecurity frameworks, policies, and privacy principles to organizational requirements.	Yes	
Knowledge of endpoint protection technologies and techniques.	Yes	
Experience working with Windows, UNIX, and Linux operating systems.	Yes	
Develops and/or delivers security awareness and training material to employees.	No	Set up meeting with IT to go over goals and expectations of security awareness and training program. Collaborate with HR to track employee engagement. Follow up with vendor for modules on phishing campaigns and data classification.

2.5 Document technical skills required for *future* work roles

2.5 Technical Skills Workbook

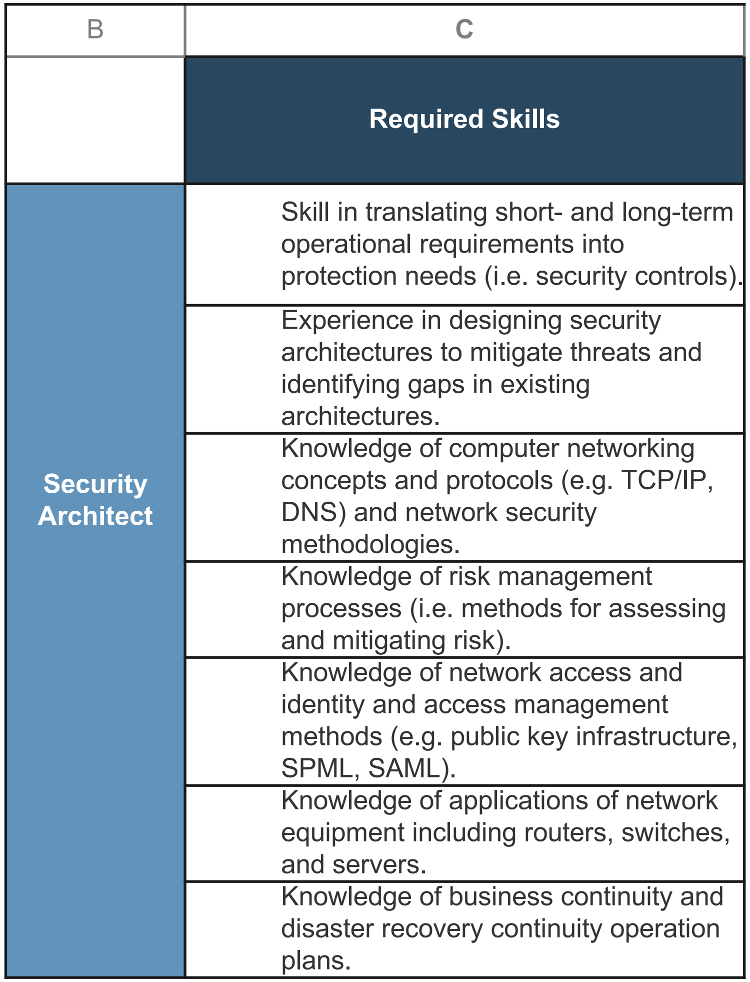
Review the *Current Workforce Skills Assessment* tool and make note of areas where your organization is lacking.

1. For those missing or immature skills, ask yourself:
   - Does this skill overlap with a future job role?
   - Can the skill be a requirement of a future job role?
   - What is the relevance of this skill in terms of my security roadmap? How did it rank in the *Skills Gap Prioritization Tool?*

   Answers to these questions will help justify whether skill gaps in the current workforce should be carried forward into developing another future job role, merged with another future job role, or addressed with training.

Referring to Exercise 2.1, use Tab 2 in the *Technical Skills Workbook* to:

2. Input the future job roles in Column B.
3. Adjacent to each job role, input the required skills in Column C.
4. Record in Column I whether an existing employee has the skill. Reference the [*Current Workforce Skills Assessment*]() tool for clarification.



B	C
	Required Skills
Security Architect	Skill in translating short- and long-term operational requirements into protection needs (i.e. security controls).
	Experience in designing security architectures to mitigate threats and identifying gaps in existing architectures.
	Knowledge of computer networking concepts and protocols (e.g. TCP/IP, DNS) and network security methodologies.
	Knowledge of risk management processes (i.e. methods for assessing and mitigating risk).
	Knowledge of network access and identity and access management methods (e.g. public key infrastructure, SPML, SAML).
	Knowledge of applications of network equipment including routers, switches, and servers.
	Knowledge of business continuity and disaster recovery continuity operation plans.

PHASE 3

Develop a Skills Sourcing Plan for Future Work Roles

Phase 3 outline

☎ **Call 1-888-670-8889** or email GuidedImplementations@InfoTech.com for more information.

Complete these steps on your own, or call us to complete a guided implementation. A guided implementation is a series of 2-3 advisory calls that help you execute each phase of a project. They are included in most advisory memberships.

Guided Implementation 3: Develop a Skills Sourcing Plan for Future Work Roles

Proposed Time to Completion: 3 weeks

Steps 3.1-3.2: Understand and Define the Factors That Influence the Skills Sourcing Plan

Start with an analyst kick-off call:

- Discuss the five key factors for acquiring needed skills.
- Discuss options for sourcing a skill.

Then complete these activities…

- Adapt impact scoring scales for five key factors.
- Apply impact scores to each skill need.
- Review skill radar charts.

With these tools & templates:

Technical Skills Workbook, Tabs 1-3

Steps 3.3-3.4: Decide How to Acquire Skills

Review findings with analyst:

- Review the *Technical Skills Workbook* key factor impact scoring and skill radar charts.

Then complete these activities…

- Discuss how skill radar charts are used to decide your sourcing plan.
- Decide how skills will be acquired.
- Review sourcing decisions.

With these tools & templates:

Technical Skills Workbook, Tabs 2-5

Phase 3 Results & Insights:

- Create an impact scale for five key factors that reflects your organizational strategy, initiatives, and pressures.
- Apply the impact scale to needed skills to identify the preferred method of skills acquisition based on the characteristics of need.

3.1 Review the five key factors for skills acquisition

The overall **characteristics** of the skills you need will determine the hiring manager’s preferred method for skills acquisition.

Frequency: How often will this skill be deployed to provision, configure, run, pause, or destroy workloads?

Data Criticality: What is the most sensitive data classification level processed by the systems that support the skill?

Urgency: How soon do we need to add this skill to our team’s toolbox? What is the required time-to-value?

Durability: How long will this skill be needed in your environment? Is it required just once or is it crucial to regular operations?

Availability: Do these skills need to be available around the clock or only during office hours?

3.1 Adapt impact scoring scales for the five key characteristics

3.1 Technical Skills Workbook

1 Tab 1: Scoring Scales

Review the **impact scoring scales** for each key factor in the *Technical Skills Workbook*. Modify the scales to reflect your environment and organizational parameters (e.g. adjust the "Urgency" time scale to reflect your schedule).

Note: For data criticality, impact levels are assigned based on the highest data classification level associated with the system and process. For example, if the system affected by the skill is associated with mostly public data but also a few top secret files, we would assign the impact level of that skill as "Very High."

Key Factor – Impact Scoring Scales

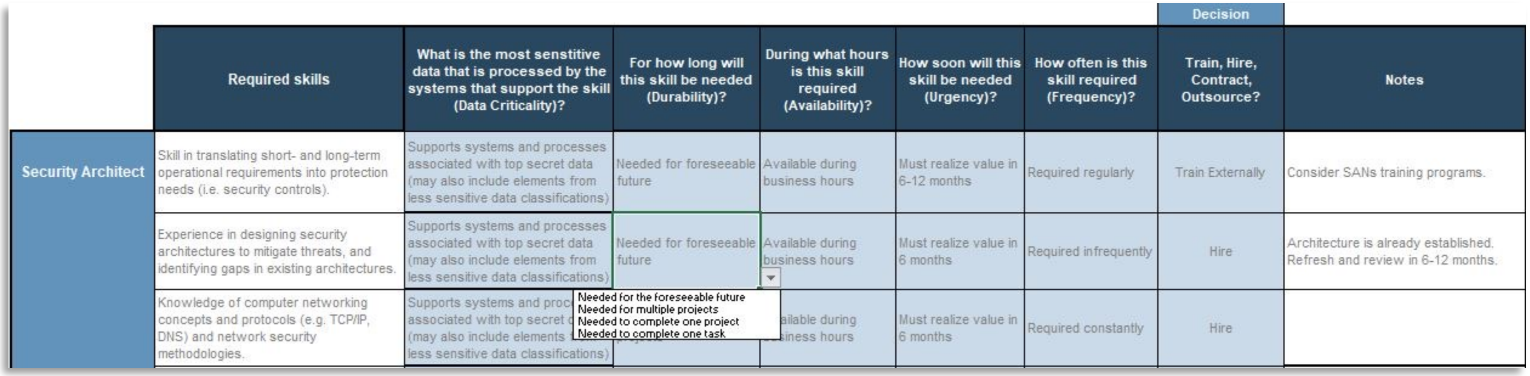
Impact Level	Data Criticality	Durability	Availability	Urgency	Frequency
Very High	Supports systems and processes associated with *top secret data* (may also include elements from less sensitive data classifications).	Needed for foreseeable future	Available 24/7	Realize value in 6 months	Required constantly
High	Supports systems and processes associated with *confidential data* (may also include elements from less sensitive data classifications).	Needed for multiple projects	Available most evenings and weekends	Realize value in 6-12 months	Required regularly
Medium	Supports systems and processes associated with *internal data* (may also include elements from less sensitive data classifications).	Needed to complete one project	Available some evenings and weekends	Realize value in 12-18 months	Required infrequently
Low	Supports systems and processes associated with only *public data*.	Needed to complete one task	Available during business hours	Realize value in > 18 months	Required rarely

3.1 Assign impact score to skills

3.1 Technical Skills Workbook

2 Tab 2: Acquire Skills

Use drop-down boxes to record the characteristics of need for each skill and each role.



							Decision	
	Required skills	What is the most senstitive data that is processed by the systems that support the skill (Data Criticality)?	For how long will this skill be needed (Durability)?	During what hours is this skill required (Availability)?	How soon will this skill be needed (Urgency)?	How often is this skill required (Frequency)?	Train, Hire, Contract, Outsource?	Notes
Security Architect	Skill in translating short- and long-term operational requirements into protection needs (i.e. security controls).	Supports systems and processes associated with top secret data (may also include elements from less sensitive data classifications)	Needed for foreseeable future	Available during business hours	Must realize value in 6-12 months	Required regularly	Train Externally	Consider SANs training programs.
	Experience in designing security architectures to mitigate threats, and identifying gaps in existing architectures.	Supports systems and processes associated with top secret data (may also include elements from less sensitive data classifications)	Needed for foreseeable future	Available during business hours	Must realize value in 6 months	Required infrequently	Hire	Architecture is already established. Refresh and review in 6-12 months.
	Knowledge of computer networking concepts and protocols (e.g. TCP/IP, DNS) and network security methodologies.	Supports systems and processes associated with top secret data (may also include elements from less sensitive data classifications)	[illegible]	Available during business hours	Must realize value in 6 months	Required constantly	Hire	

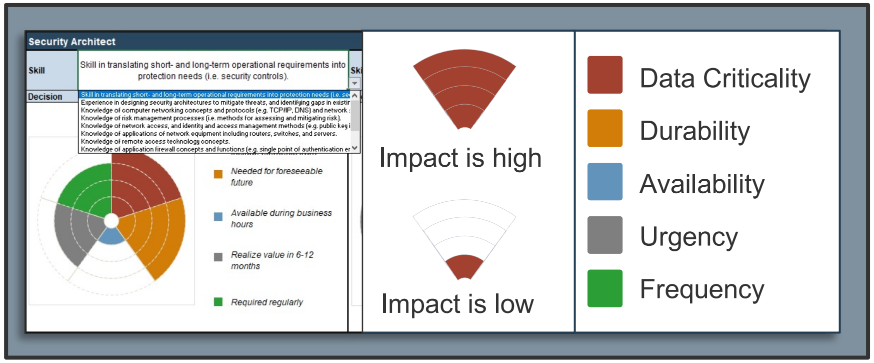
Needed for the foreseeable future
Needed for multiple projects
Needed to complete one project
Needed to complete one task

3 Tab 3: Radar Charts

Responses from Tab 2 are visualized in Tab 3.

- Use the drop-down box to review different skills in each role.

This diagram provides an at-a-glance illustration of impacts driving the acquisition decision for each skill.



Security Architect

Skill: Skill in translating short- and long-term operational requirements into protection needs (i.e. security controls).

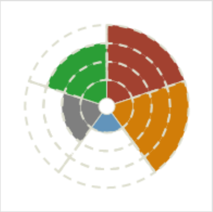
Decision

Skill in translating short- and long-term operational requirements into protection needs (i.e. se
Experience in designing security architectures to mitigate threats, and identifying gaps in existir
Knowledge of computer networking concepts and protocols (e.g. TCP/IP, DNS) and network :
Knowledge of risk management processes (i.e. methods for assessing and mitigating risk).
Knowledge of network access, and identity and access management methods (e.g. public key i
Knowledge of applications of network equipment including routers, switches, and servers.
Knowledge of remote access technology concepts.
Knowledge of application firewall concepts and functions (e.g. single point of authentication er

3.2 Explore your options for sourcing skills – hire or train (Tab 3)

Hire

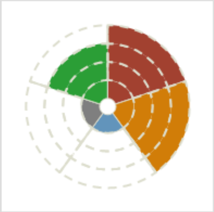
Go to market for new staff when internal talent is unavailable to fulfill needed core roles and skills.



- Moving through the hiring process, onboarding the new employee, and getting to value **can take months.** Ensure sufficient lead time to get-to-value for needed skills.
- 45% of organizations take at least three months to fill a cybersecurity vacancy.[1]
- 26% of enterprises take more than six months to fill cybersecurity and information security positions.[1]

Train

Acquiring new skills via training can improve staff performance and add skills for future opportunities.

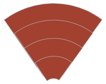


- Staff need to set aside time for training and get-to-value on new skills needed for a particular initiative.
- The level of training offered by the organization was rated among the top three **motivating factors for recruiting and retaining cybersecurity employees.**[2]
- Look for high-quality training programs that teach transferrable skills. SANs and eLearnSecurity offer role-specific training programs aligned with the NCWF.

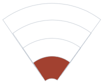
Info-Tech **Best Practice**

Deciding between hiring and training for *new* skills often comes down to your staff's available time. Use time-tracking tools to decide whether capacity is available for training new skills – but ensure opportunities are regularly available for continuous improvement.

Needs Characteristics Legend



Impact is high



Impact is low

🟥 Data Criticality
🟧 Durability
🟦 Availability
⬛ Urgency
🟩 Frequency

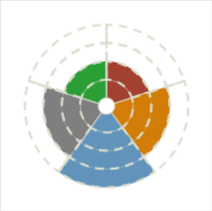
[1] Cybersecurity Nexus, 2018
[2] McAfee, 2016

3.2

Explore your options for sourcing skills – outsource or contract (Tab 3)

Outsource

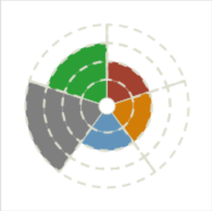
Ensure you have enough time to effectively plan an outsourcing agreement.



- Outsourcing to acquire skills can be a viable option for even core skills and critical systems. The more critical the systems, the more planning and lead time is required.
- Signing multiple statements of work (SOWs) with the same provider can be an effective way to perforate your outsourcing agreement, providing you with the option to tear off underperforming services.
- Outsourcing can ease the workload on current cybersecurity staff, allowing them to address more pressing matters that require human intervention.
- Using a managed security service provider (MSSP) may be more cost effective than hiring a team of security experts.

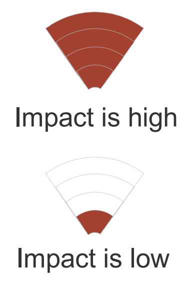
Contract

Find flex or contract staff when specialized skills are needed urgently.



- Finding a suitable contractor is generally a faster process than hiring new staff, and an urgent need on a committed project can warrant using a contractor.
- Using a contractor is lower risk because it's easier to end the arrangement.
- Contracting is more expensive on an hourly basis than a full-time employee, so contracting usually isn't a good option for meeting ongoing needs.
- Ensure documentation is part of the deliverables.
- If you need more systematic knowledge transfer for skills on an ongoing basis, be very clear on expectations about training for your staff, as many contractors are not resourced to provide training, and inexperienced contractors may not be comfortable being shadowed by your staff.

Needs Characteristics Legend



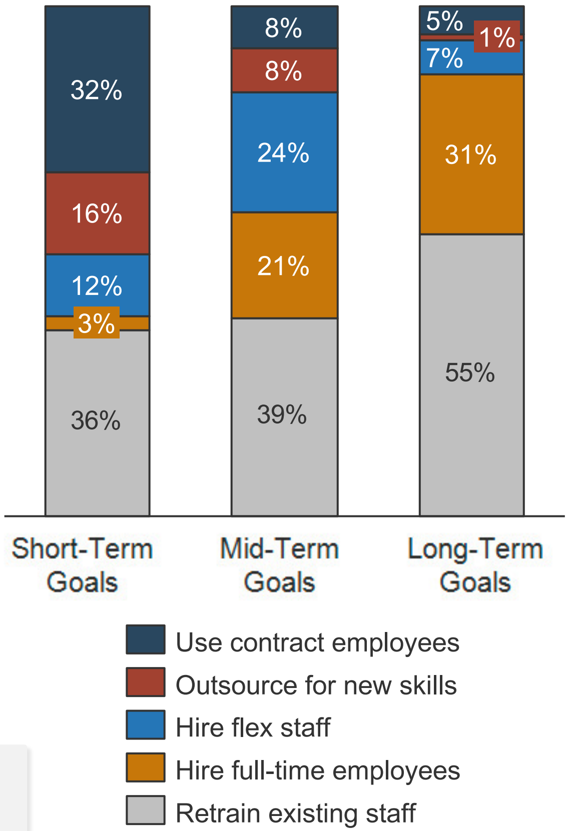
🟥 Data Criticality
🟧 Durability
🟦 Availability
⬛ Urgency
🟩 Frequency

3.2 Training and hiring tend to be long-term strategies

Organizations that require skills for short-term goals are more likely to **contract or outsource** than those with longer projects.

- Organizations always **prefer to leverage the skills of existing staff** when searching for new competencies. However, when it comes to **required skills that have near-term significance,** there is increased interest in using contract employees or hiring flex staff.
- When a skill is both **urgent** and **critical** (supports mission critical systems or core processes), organizations tend to hire contract staff.
- Translate the short-term assignment into long-term value by making **knowledge transfer,** as-built documentation, and seeding the knowledgebase required deliverables in the SOW.

How Organizations Plan to Acquire New Skills



Source: Info-Tech Research Group

Info-Tech **Insight**

If your organization is scrambling to acquire new skills, you likely won't find them internally and you won't fully leverage the abilities of your current staff. Plan ahead so you can meet skill needs inside your organization.

3.2

If you choose to train, offering development and certification opportunities helps recruit and retain staff

SANS and GIAC Certifications have partnered with the NCWF to align 35 security courses and certifications to all roles within the NCWF.

Popular InfoSec Certifications

1. CISSP: Certified Information Systems Security Professional
2. CISM: Certified Information Security Manager
3. CISA: Certified Information Systems Auditor
4. CEH: Certified Ethical Hacker
5. CompTIA Security+
6. GSEC: SANS GIAC Security Essentials

eLearnSecurity provides training paths designed for individuals wanting to gain proficiency in industry standard roles outlined in the NCWF. Training paths support the roles of:

- System Administrator
- Vulnerability Assessment Analyst
- Cyber Defense Incident Responder
- Law Enforcement/Counterintelligence Forensics Analyst
- Cyber Defense Forensics Analyst
- Cyber Instructor
- Secure Software Assessor
- Exploitation Analyst

3.2 Outsourcing services to an MSSP is a complex decision

When cybersecurity professionals are scarce internally and externally, outsourcing responsibilities to an MSSP is a very popular option.

Contracts with MSSPs tend to be large scale and long term. Therefore, conducting thorough research and analysis on potential MSSPs is imperative.

Several factors go into choosing an MSSP. Some examples are:

1. **Talent, expertise, and reputation.**
2. **Services offered:** Do the services align to your organization's security requirements, compliance needs, and risk toleration?
3. **Budget constraints:** How does the MSSP charge for services?
4. **Integration**: How will the MSSP integrate with the existing infrastructure?

Increase your chances of success:

- Clearly define your goals, requirements, and success metrics for the acquisition.
- Solicit proposals with a thorough and right-sized RFP.
- Standardize your selection process and get multiple staff to score responses.
- Conduct vendor due diligence.

Info-Tech **Best Practice**

Leverage Info-Tech's blueprint *Develop Your Security Outsourcing Strategy* to help you outsource the right services with the right MSSP.

3.3 Determine how to acquire needed skills

3.3 Technical Skills Workbook

	High Impact
Contract	**Urgency:** Contracting can help you acquire skills that are required in the very short term, but enough time to conduct due diligence is still required.
Outsource	**Availability:** Skills may be needed during extended business hours. **Urgency:** Outsourcing can meet the needs of urgent projects, but appropriate due diligence is required.
New Hire	**Data Criticality:** Required for systems and processes associated with top secret and/or confidential information. **Durability:** The skill is needed for the foreseeable future. **Frequency:** The skill is needed often.
Training	**Data Criticality:** Required for systems and processes associated with top secret and/or confidential information. **Durability:** The skill is needed for the foreseeable future. **Frequency:** The skill is needed often.

1. Review **very high** and **high impacts** in the radar charts on Tab 3 and compare them with the guidance table on the left. Eliminate nonviable acquisition options.

2. If you can't make a decision based on high-impact factors alone, review the **medium impact** guidance table below.

	Medium Impact
Contract	**Availability:** Skills may be needed during extended business hours. **Data Criticality:** May support systems or processes associated with internal information.
Outsource	**Durability:** Needed for several projects. **Data Criticality:** May support systems or processes associated with internal information.
New Hire	**Urgency:** The skills are required to deliver value in the medium term; sufficient time is available to onboard.
Training	N/A

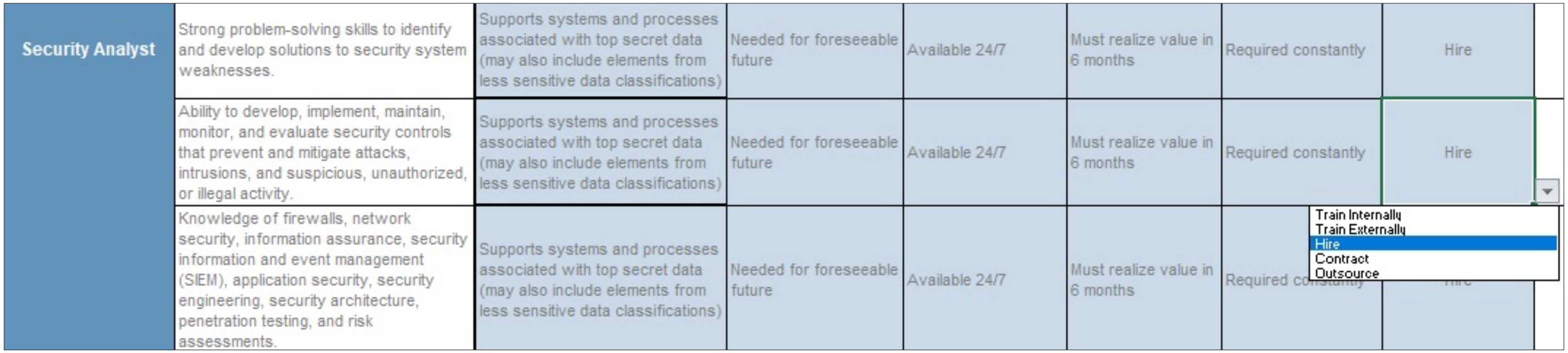
Record the decision to acquire skills in your copy of the *Technical Skills Workbook*

3.3 Technical Skills Workbook

3 Review the low impact table if needed.

4 Record your decisions in **Tab 2: Acquire Skills.** Use the drop-down boxes in the Decision Column to identify whether you plan to hire, train, contract, or outsource.

	Low Impact
Contract	**Data Criticality:** May support systems or processes associated with public data. **Durability:** The skill is not needed long term. **Frequency:** The skill may be needed regularly or infrequently.
Outsource	**Data Criticality:** May support systems or processes associated with public data. **Frequency:** May be needed regularly or infrequently.
New Hire	**Availability:** Skills are usually needed only during normal business hours.
Training	**Availability:** Skills are usually needed only during normal business hours. **Urgency:** The required time-to-value for this skill is long.



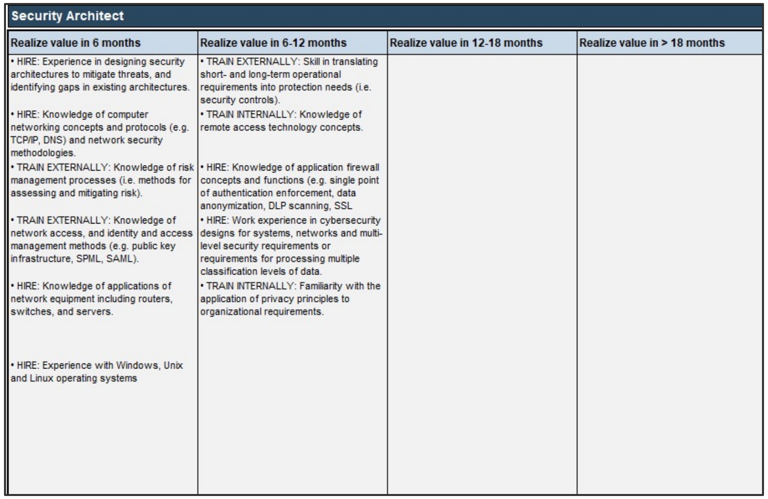
Security Analyst	Strong problem-solving skills to identify and develop solutions to security system weaknesses.	Supports systems and processes associated with top secret data (may also include elements from less sensitive data classifications)	Needed for foreseeable future	Available 24/7	Must realize value in 6 months	Required constantly	Hire
	Ability to develop, implement, maintain, monitor, and evaluate security controls that prevent and mitigate attacks, intrusions, and suspicious, unauthorized, or illegal activity.	Supports systems and processes associated with top secret data (may also include elements from less sensitive data classifications)	Needed for foreseeable future	Available 24/7	Must realize value in 6 months	Required constantly	Hire
	Knowledge of firewalls, network security, information assurance, security information and event management (SIEM), application security, security engineering, security architecture, penetration testing, and risk assessments.	Supports systems and processes associated with top secret data (may also include elements from less sensitive data classifications)	Needed for foreseeable future	Available 24/7	Must realize value in 6 months	Required constantly	Hire

3.4 Review decision

3.4 Technical Skills Workbook

Tab 4: Skills Map

Use this reporting tab to review what skills are needed and when and how you plan to acquire them for each identified role.

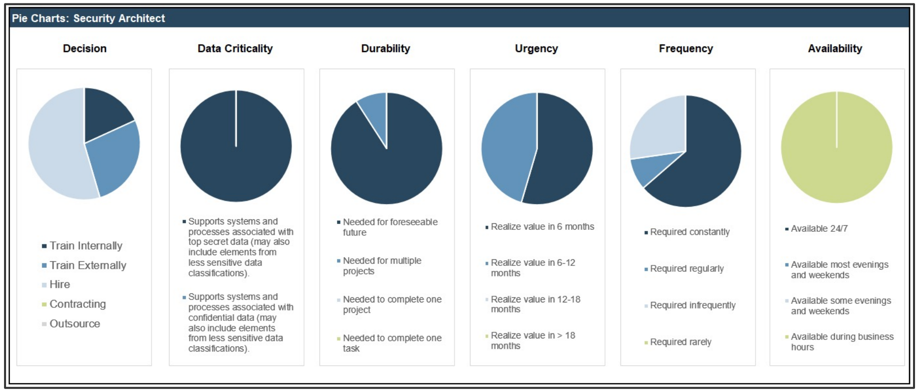


Security Architect

Realize value in 6 months	Realize value in 6-12 months	Realize value in 12-18 months	Realize value in > 18 months
• HIRE: Experience in designing security architectures to mitigate threats, and identifying gaps in existing architectures. • HIRE: Knowledge of computer networking concepts and protocols (e.g. TCP/IP, DNS) and network security methodologies. • TRAIN EXTERNALLY: Knowledge of risk management processes (i.e. methods for assessing and mitigating risk). • TRAIN EXTERNALLY: Knowledge of network access, and identity and access management methods (e.g. public key infrastructure, SPML, SAML). • HIRE: Knowledge of applications of network equipment including routers, switches, and servers. • HIRE: Experience with Windows, Unix and Linux operating systems	• TRAIN EXTERNALLY: Skill in translating short- and long-term operational requirements into protection needs (i.e. security controls). • TRAIN INTERNALLY: Knowledge of remote access technology concepts. • HIRE: Knowledge of application firewall concepts and functions (e.g. single point of authentication enforcement, data anonymization, DLP scanning, SSL • HIRE: Work experience in cybersecurity designs for systems, networks and multi-level security requirements or requirements for processing multiple classification levels of data. • TRAIN INTERNALLY: Familiarity with the application of privacy principles to organizational requirements.		

Tab 5: Pie Charts

Use this reporting tab to review decisions, and the impact of different factors, across each role.



Info-Tech Insight

A skills gap will always exist to some degree. Regularly assessing the projected skills gap will allow you to proactively avoid security backlogs and business interruption.

3.4

Establish baseline metrics around addressing the skills gap

Baseline metrics will improve through:

1. Aligning security initiative skill needs with workforce roles.
2. Being aware of what and where skills gaps exist in the workforce.
3. Understanding how to acquire skills based on the five key factors.

Metric Description	Current Metric	Future Goal
Total number of IT security employees	5	8
Total number of security initiatives completed per year	20	25
Total number of security initiatives canceled per year	5	0
Yearly turnover total in IT security	2	1
Average hours billed at overtime rate per IT employee	6	2
Other metric		
Other metric		
Other metric		
Other metric		
Other metric		
Other metric		

Example metrics to use

Insight breakdown

Plan for the inevitable.

- All industries are expected to be affected by the talent gap in the coming years. Plan to address the skills required for the future state of your organization.
- Identify skills needed in the organization to support your security roadmap initiatives and align them with your workforce requirements to provide the link between your workforce and cybersecurity strategy.

Base skills acquisition decisions on the five key factors to define skill needs.

- Create an impact scale for the five key factors (data criticality, durability, availability, urgency, frequency) that reflects your organizational strategy, initiatives, and pressures.
- Apply the impact scale to needed skills to identify the preferred method of skills acquisition based on the characteristics of need.

A skills gap will always exist to some degree.

- The threat landscape is constantly changing, and your workforce's skill sets should as well.
- Regularly assessing the projected skills gap will allow you to proactively avoid security backlogs and business interruption.

Summary of accomplishment

Knowledge Gained

- The importance of aligning security initiative skill needs to workforce requirements.
- The options that exist for sourcing skills.
- How to source needed skills.

Processes Optimized

- Identify the skills your organization needs to support your security initiatives.
- Align the skills required by your future initiatives to your workforce.
- Acquire needed skills based on a systematic methodology.

Deliverables Completed

- *Security Initiative Skills Guide*
- *Skills Gap Prioritization Tool*
- *Current Workforce Skills Assessment*
- *Technical Skills Workbook*

Research contributors and experts

Amanda Bluett
Head of Cyber Defence and Assurance
CBRE – APAC

Amanda is an enthusiastic Information System Risk and Security practitioner. She has 18 years of experience and has been involved in assisting some of the world's largest businesses in all areas of the cybersecurity realm. Specialty areas include investigations, mobile forensics, internet intelligence, information system audit, information system analysis and risk management, information system security architecture, information governance and management, eDiscovery, security strategy, and enterprise security.

Eldon Sprickerhoff
Chief Innovation Officer
eSentire, Inc.

Eldon is the founder and the Chief Innovation Officer at eSentire. With over 25 years of tactical information security experience, he has set the future vision and direction for security technology within the company, defining operational security best practices and overseeing the security posture on behalf of the customers. He holds several security industry certifications (including CISSP and CISA) and is considered to be a subject matter expert in information security analysis, particularly in regards to financial services firms on the buy side.

Research contributors and experts

Anja Adam
Manager of Information Security – IT Risk & Compliance
De Lage Landen International B.V.

Four Anonymous Contributors

Related Info-Tech research

Build an Information Security Strategy

Tailor best practices to effectively manage information security.

Build a Strategic Workforce Plan

Have the right people, in the right place, at the right time.

Bibliography

Hancock, Geoff, et al. *Cybersecurity Workforce Handbook: A Practical Guide to Managing Your Workforce.* Council on CyberSecurity. 2014. Web.

Identity Theft Resource Center. “2017 Annual Data Breach Year-End Review.” *CyberScout*. 2018. Web.

ISACA. “State of Cybersecurity 2018.” *Cybersecurity Nexus*. 2018. Web.

(ISC)^2. “Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: (ISC)^2 Cybersecurity Workforce Study, 2018.” *(ISC)^2.* 2018. Web.

McAfee. “Hacking the Skills Shortage.” *McAfee*. July 2016. Web.

Morgan, Steve. “Cybersecurity Unemployment Rate Drops to Zero Percent.” *Cybersecurity Ventures*. 19 Sept. 2016. Web.

Newhouse, William, et al. “NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.” *NIST.* Aug. 2017. Web.

Oltsik, Jon. “Research Suggests Cybersecurity Skills Shortage Is Getting Worse.” *CSO.* 11 Jan. 2018. Web.

Oltsik, Jon. “The Life and Times of Cybersecurity Professionals.” *Enterprise Strategy Group*. Nov. 2017. Web.

Sullivan, John. “VUCA: The New Normal for Talent Management and Workforce Planning.” *ERE Media.* 16 Jan. 2012. Web.