

JUST TELL ME WHAT I NEED TO KNOW...

CYBERSECURITY Q & A WORKBOOK

CLEAR ANSWERS. | PRACTICAL INSIGHTS. | ESSENTIALS ONLY.



LEARN.
UNDERSTAND.
APPLY.
STAY SECURE.



100+
QUESTIONS



REAL-WORLD
SCENARIOS



DETAILED
EXPLANATIONS



KEY CONCEPTS
MADE SIMPLE



TEST YOUR
KNOWLEDGE



BUILD SKILLS.
THINK LIKE
A DEFENDER.



PRACTICE WITH
REAL-WORLD
EXAMPLES



IMPROVE.
PREPARE.
SUCCEED.

Just Tell Me What I Need To Know
Cybersecurity Q&A Workbook

A Security Architect's Practical Guide

Belshaw Consulting

Copyright Notice

This book is an independent educational work. Any company names, product names, trademarks, service marks, technologies, standards, frameworks, methodologies, or registered trademarks mentioned in this publication are the property of their respective owners. Their inclusion is for identification, educational, and illustrative purposes only and does not imply any affiliation with, endorsement by, or sponsorship from the respective owners.

Technology, products, standards, regulations, certifications, security guidance, and industry best practices evolve over time. Readers should consult current vendor documentation, official standards publications, applicable regulations, and their organization's policies and procedures before implementing any recommendations or making technical, security, or business decisions.

Copyright © 2026 Belshaw Consulting

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, transmitted, or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher, except for brief quotations used in reviews or scholarly works as permitted by applicable copyright law.

Table of Contents

Introduction	5
Security and Risk Management	7
Understand, adhere to, and promote professional ethics	7
Understand and apply CIA security concepts	17
Evaluate and apply security governance principles	26
Understand legal, regulatory, and compliance issues.....	43
Understand requirements for investigation types	64
Develop, document, and implement security policy and standards	75
Identify, analyze, assess, prioritize BCDR	85
Enforce personnel security policies and procedures	96
Understand and apply risk management concepts	117
Understand and apply threat modeling concepts	153
Supply chain risk management (SCRM) concepts.....	170
Security awareness, education, and training	190
Asset Security.....	211
Identify and classify information and assets.....	211
Establish information and asset handling requirements	232
Provision information and assets securely.....	242
Manage data lifecycle	262
Ensure appropriate asset retention	300
Determine data security controls	310
Security Architecture and Engineering	357
Manage engineering processes	357
Understand Security models.....	395
Select controls based on security requirements.....	436
Understand security capabilities of Information Systems	446
Assess and mitigate vulnerabilities	464
Select and determine cryptographic solutions	533
Understand methods of cryptanalytic attacks	621
Apply security principles to site and facility design	658
Design site and facility security controls.....	674
Manage the information system lifecycle	690

Communication and Network Security	707
Apply secure design principles in network architectures.....	707
Secure network components.....	788
Implement secure communication channels	841
Identity and Access Management	905
Control physical and logical access to assets.....	905
Design identification and authentication strategy	925
Federated identity with a third-party service.....	963
Implement and manage authorization mechanisms.....	981
Manage the identity and access lifecycle	1044
Implement authentication systems.....	1082
Security Assessment and Testing.....	1102
Assessment, test, and audit strategies	1102
Conduct security control testing	1125
Collect security process data	1168
Analyze test output and generate report	1212
Conduct or facilitate security audits.....	1234
Security Operations	1256
Understand and comply with investigations	1256
Conduct logging and monitoring activities.....	1276
Perform configuration management.....	1297
Apply foundational security operations concepts.....	1318
Apply resource protection.....	1338
Conduct incident management	1360
Detection and preventative measures	1381
Patch and vulnerability management.....	1400
Change management processes.....	1420
Implement recovery strategies.....	1440
Implement disaster recovery processes.....	1459
Test disaster recovery plans.....	1479
Business Continuity (BC) planning	1499
Implement and manage physical security	1519
Personnel safety and security.....	1538

Software Development Security	1558
Integrate security in the SDLC	1558
Security controls in software development	1602
Assess effectiveness of software security	1670
Security impact of acquired software	1694
Secure coding guidelines and standards.....	1756
Final Words	1807

Introduction

Welcome to the ****Just Tell Me What I Need To Know - Cybersecurity Q&A Workbook****.

If you've read any of the other books in the **Just Tell Me What I Need To Know...** series, you already know the philosophy behind them: cut through the noise, skip the unnecessary complexity, and focus on the knowledge that professionals actually need to understand and apply. Each book is designed to provide a practical, concise, and vendor-neutral guide to a specific cybersecurity topic, helping you build both confidence and competence without requiring you to read a thousand-page reference manual.

This workbook is different—but it has the same mission.

Rather than introducing new concepts, the ****Cybersecurity Q&A Workbook**** helps you reinforce and apply what you've already learned. Think of it as the gym for your cybersecurity brain. Reading builds knowledge; answering questions builds recall, confidence, and the ability to explain concepts when it matters most.

Whether you're preparing for a certification exam, studying for a college course, interviewing for a cybersecurity position, training new team members, or simply checking your own understanding, this workbook provides an opportunity to test yourself across the broad range of topics that make up modern cybersecurity.

The questions span foundational principles, security technologies, governance, cloud security, networking, identity and access management, risk management, incident response, threat management, Zero Trust, DevSecOps, artificial intelligence, and many other areas covered throughout the series. Some questions are straightforward and designed to reinforce key concepts. Others require you to think critically, connect ideas from multiple domains, and apply your knowledge to realistic scenarios—the kind of thinking expected of cybersecurity professionals every day.

One of the strengths of the **Just Tell Me What I Need To Know...** series is that each book stands on its own while also complementing the others. The workbook follows the same philosophy. It can be used independently as a general cybersecurity study guide, but it becomes even more valuable when paired with the other books in the series. After reading a topic such as Cloud Security, Zero Trust, Risk Assessment, Threat Management, or DevSecOps, return to this workbook and challenge yourself to recall the important concepts without immediately looking up the answers. That process of active recall is one of the most effective ways to retain information over the long term.

Don't worry if you can't answer every question on your first attempt. The goal isn't perfection—it's progress. Every question you miss highlights an opportunity to strengthen your understanding. In many cases, discovering what you don't know is just as valuable as confirming what you do.

Cybersecurity is a field that changes continuously. New technologies emerge, attackers develop new techniques, regulations evolve, and best practices mature. The most successful professionals aren't the ones who memorize every fact—they're the ones who develop a strong foundation, think critically, and continue learning throughout their careers. This workbook is designed to help you build those habits.

So, grab a pen, challenge yourself, and don't be afraid to get a few answers wrong along the way. After all, the only bad question is the one you never ask—and the only missed learning opportunity is the one you never attempt. Let's see how much you really know.

KNOWLEDGE ISN'T ENOUGH. YOU HAVE TO BE ABLE TO APPLY IT.

Reading about cybersecurity is only the beginning. The real challenge is thinking through security problems, making sound decisions, and explaining why your solution is the right one.

The **Just Tell Me What I Need to Know - Cybersecurity Q&A Workbook** is the companion to *Just Tell Me What I Need to Know... Cybersecurity*, designed to help you reinforce your knowledge through practical questions, realistic scenarios, and interview-style exercises.

INSIDE YOU'LL FIND:

- ✓ Hundreds of review questions covering every major cybersecurity domain
- ✓ Multiple-choice, true/false, and short-answer exercises
- ✓ Scenario-based challenges that develop critical thinking
- ✓ Architecture, risk, and decision-making exercises
- ✓ Interview preparation questions with practical insights
- ✓ Exercises that connect technical concepts to real business problems
- ✓ A valuable study companion for students, professionals, and certification candidates

Whether you're preparing for an interview, studying for a certification, transitioning into cybersecurity, or simply wanting to strengthen your understanding, this workbook helps you move beyond memorization and develop the judgment that successful cybersecurity professionals rely on every day.



With a total of 1770 questions and detailed explanations of the answers, this book engages students directly, requiring them to think, respond, and participate actively. The specificity and level of detailed analysis in the explanations makes the book a perfect independent companion book.



USE IT ON
YOUR OWN



IN STUDY
GROUPS



IN THE
CLASSROOM



AS A PRACTICAL
COMPANION



TO THE REST OF THE
JUST TELL ME WHAT
I NEED TO KNOW...
SERIES



**KNOWING THE ANSWER IS IMPORTANT.
UNDERSTANDING WHY IT'S THE ANSWER
IS WHAT BUILDS EXPERTISE.**