

JUST TELL ME WHAT I NEED TO KNOW...

POLICIES & PROCEDURES



CLEAR GUIDANCE. CONSISTENT ACTION.
STRONGER SECURITY.



DEFINE

Establish clear objectives and scope aligned to business and security goals.



RESEARCH

Understand requirements, standards, and regulatory obligations.



DRAFT

Write clear, concise, and actionable policies and procedures.



REVIEW

Collaborate with stakeholders and subject matter experts for accuracy.



APPROVE

Obtain formal approval and ensure alignment with governance requirements.



- ✓ USE CLEAR, CONSISTENT LANGUAGE
- ✓ BE SPECIFIC, NOT VAGUE
- ✓ DEFINE ROLES & RESPONSIBILITIES
- ✓ INCLUDE EXAMPLES & GUIDANCE
- ✓ ENSURE ENFORCEABILITY & COMPLIANCE
- ✓ KEEP IT CURRENT AND RELEVANT

WELL-WRITTEN POLICIES & PROCEDURES:

- ✓ REDUCE RISK
- ✓ ENSURE COMPLIANCE
- ✓ PROMOTE CONSISTENCY
- ✓ IMPROVE DECISION MAKING
- ✓ SUPPORT OPERATIONAL EXCELLENCE



PLAN



WRITE



REVIEW



APPROVE



PUBLISH



MONITOR & UPDATE

Just Tell Me What I Need To Know
Policies & Procedures

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
Part I — Governance Foundations	7
Chapter 1 — Introduction to Security Governance	7
Chapter 2 — Policy Frameworks	13
Chapter 3 — Document Hierarchy	20
Part II — Writing Effective Policies	29
Chapter 4 — Policy Development	29
Chapter 5 — Policy Lifecycle	36
Chapter 6 — Standards and Baselines	44
Part III — Enterprise Security Policies	53
Chapter 7 — Identity & Access Management Policies	53
Chapter 8 — Data Protection Policies	60
Chapter 9 — Infrastructure & Platform Policies	69
Chapter 10 — Secure Development Policies	77
Chapter 11 — Operational Security Policies	85
Part IV — Procedures & Operational Guidance	94
Chapter 12 — Developing Procedures	94
Chapter 13 — Operational Playbooks	101
Chapter 14 — Administrative Processes	110
Part V — Compliance & Governance	119
Chapter 15 — Regulatory Compliance	119
Chapter 16 — Policy Governance	128
Chapter 17 — Building a Security Governance Program	135
Part VI — Practical Governance	145
Chapter 18 — Policy Templates	145
Chapter 19 — Standards, Procedures & Checklists	155
Chapter 20 — Building a Governance Library	164
Appendices	174
Appendix A — Security Policy Development Checklist	174
Appendix B — Policy Template	183
Appendix C — Standard Template	191

Appendix D — Baseline Template	200
Appendix E — Procedure Template	209
Appendix F — Work Instruction Template	218
Appendix G — Security Playbook Template	227
Appendix H — Policy Review Checklist.....	238
Appendix I — Document Approval Workflow.....	247
Appendix J — Governance Maturity Model	257
Appendix K — Security Governance RACI Guide	267
Appendix L — Policy-to-Framework Crosswalk	276
Appendix M — Common Security Policy Library	319
Appendix N — Security Governance Interview Questions	327
Appendix O — Recommended Reading	363

Introduction

Every successful cybersecurity program is built on more than technology.

Firewalls, endpoint protection, cloud security, identity management, and monitoring tools all play important roles, but without clear policies, well-defined standards, documented procedures, and consistent governance, even the best technical controls become difficult to implement, manage, and audit. Technology changes rapidly, but good governance provides the structure that keeps security programs effective, repeatable, and aligned with business objectives.

Unfortunately, policies and procedures are often viewed as little more than paperwork created to satisfy auditors or regulatory requirements. In reality, they define how an organization operates, how decisions are made, how responsibilities are assigned, and how security expectations are communicated across the enterprise. Well-written governance documents improve consistency, reduce risk, support compliance, and provide a foundation for continuous improvement.

That's where this book comes in.

The Just Tell Me What I Need to Know... series is designed to cut through the complexity and focus on the knowledge professionals actually need. Rather than overwhelming you with legal language, regulatory jargon, or hundreds of pages of templates, each book delivers practical, real-world concepts in a clear, concise, and easy-to-understand format.

This book focuses on Policies & Procedures—the governance documents that establish expectations, guide technical implementation, and support effective security operations. You'll learn the differences between policies, standards, baselines, guidelines, procedures, work instructions, playbooks, and checklists; how to develop and maintain each type of document; and how they work together to create a mature, well-governed cybersecurity program.

Unlike books that focus solely on compliance or documentation for its own sake, this book emphasizes practical governance. It explains how organizations build policy frameworks, manage exceptions, support audits, communicate responsibilities, and maintain documentation that evolves alongside changing technologies, threats, and business requirements.

Whether you're an engineer, architect, ISSO, manager, compliance professional, auditor, executive, student, or cybersecurity leader, understanding how to develop and maintain effective policies and procedures is essential to building security programs that are both operationally effective and defensible during audits and assessments.

Most security professionals can explain encryption, firewalls, or Zero Trust. Far fewer can write a good policy, develop a standard, or create an enterprise governance framework. Yet those are exactly the skills that distinguish senior engineers, architects, ISSOs, and CISOs.

This book should answer one question:

"How do I build, document, govern, and continuously improve an enterprise cybersecurity program?"

Our goal is simple:

Give you the knowledge you need, without making you read three books to get it.

So, let's get started.

TECHNOLOGY ALONE DOESN'T SECURE AN ORGANIZATION. GOOD GOVERNANCE DOES.

Firewalls, cloud security, Zero Trust, identity management, and security monitoring are only effective when they are supported by clear policies, well-defined standards, repeatable procedures, and strong governance. Without them, security becomes inconsistent, difficult to manage, and nearly impossible to audit.

The problem? Most books on policies and procedures are either written for auditors, filled with legal jargon, or focused on compliance instead of practical implementation.

This book is different.

Just Tell Me What I Need To Know... Policies & Procedures provides a practical, business-focused guide to building and managing the governance documents that every mature cybersecurity program depends on. You'll learn how policies, standards, baselines, procedures, work instructions, playbooks, and checklists work together to transform executive direction into consistent operational practices. The book also explains governance frameworks, document lifecycles, compliance, approvals, version control, and continuous improvement—without unnecessary complexity.



INSIDE YOU'LL LEARN HOW TO:

- ✓ Build an effective security governance framework
- ✓ Write clear, enforceable policies and standards
- ✓ Develop procedures, playbooks, and operational guidance
- ✓ Manage document lifecycles, approvals, and version control
- ✓ Align governance with business objectives and regulatory requirements
- ✓ Create a centralized, maintainable governance library
- ✓ Improve compliance while reducing organizational risk
- ✓ Build a mature, scalable cybersecurity governance program



KEY GOVERNANCE DISCIPLINES



GOVERNANCE FRAMEWORKS

Establish structure, roles, and decision-making authority.



COMPLIANCE ALIGNMENT

Meet regulatory requirements and auditable controls.



STAKEHOLDER ENGAGEMENT

Collaborate across business, IT, and security teams.



DOCUMENT LIFECYCLE

Create, review, approve, version, and retire.



CONTINUOUS IMPROVEMENT

Review, measure, and improve over time.



RISK MANAGEMENT INTEGRATION

Reduce risk and strengthen resilience across the enterprise.



Whether you're a security architect, CISO, ISSO, engineer, auditor, compliance professional, project manager, consultant, or aspiring cybersecurity leader, this book gives you the practical knowledge you need to create governance documentation that **supports real-world security—not just successful audits.**



REDUCE RISK



Consistent policies and procedures reduce exposure and uncertainty.



IMPROVE EFFICIENCY

Standardized guidance saves time and supports scalability.



STRENGTHEN COMPLIANCE

Meet audit requirements with confidence and clarity.



ENABLE THE BUSINESS

Good governance supports innovation and growth.

CLEAR GUIDANCE. CONSISTENT ACTION. **STRONGER SECURITY.**

B E L S H A W C O N S U L T I N G