Tech Writing Portfolio

Style Samples v2026.1

Lisa Brown

lbanet2go@yahoo.com Macungie, PA (484) 891-1068

LISA BROWN

Tech Writing Portfolio

Style Samples v2026.1

PAGE LEFT
INTENTIONALLY
BLANK

Table of Content

PAGE LEFT
INTENTIONALLY
BLANK

LISA BROWN

Tech Writing Portfolio

Style Samples v2026.1

CONTRIBUTIONS:

Name(s)	Content Contributor(s)
Lisa Brown	Author / Tech Writer

1 Getting Started

2 About The Author

Lisa Brown is an experienced technical writer and technology professional specializing in compliance documentation, operational SOPs, and knowledge management systems. With decades of expertise in IT services, governance frameworks, and enterprise documentation, she produces clear, audit-ready content that strengthens workforce continuity, reduces risk, and supports organizational resilience.

3 Introduction

This portfolio is created to demonstrate multiple technical writing styles, including compliance-driven narratives, operational SOPs, service desk knowledge articles, and executive technical documentation. These writing standards have been applied across industries such as information technology, utilities, workforce systems, regulated compliance environments, professional services, and AI-enabled education infrastructure.

SAMPLE 1 — STANDARD OPERATING PROCEDURE (SOP)

4 SOP-001: Access Control & Privileged Account Management

4.1 Purpose

The purpose of this SOP is to ensure privileged access to critical systems is managed securely, consistently, and in compliance with organizational governance and regulatory expectations.

4.2 Scope

This procedure applies to all workforce members, contractors, and third-party vendors with administrative access to enterprise infrastructure, including identity systems, network platforms, and operational databases.

4.3 Roles & Responsibilities

Role	Responsibility
Compliance Lead	Ensures alignment with regulatory requirements
IT Security Admin	Approves and provisions privileged access
System Owner	Validates business justification
Workforce Member	Adheres to access use policies

4.4 Procedure Steps

- Request Submission
  - User submits an access request through ServiceNow with documented justification.
- **Approval Workflow**
  - System Owner reviews the request.
  - Compliance Lead verifies regulatory alignment.

- **Provisioning Controls**
  - Access is granted using least privilege principles.
  - Privileged accounts must be uniquely assigned (no shared credentials).
- **Logging and Monitoring**
  - All privileged access activity is logged and retained for audit review.
- **Quarterly Access Review**
  - Access lists are reviewed quarterly and revoked if no longer required.

4.5 Evidence Artifacts (Audit-Ready)

- Access request ticket ID
- Approval record
- Privileged account registry
- Quarterly review logs

4.6 Compliance Outcome

This SOP supports workforce accountability, reduces operational risk, and ensures defensible access governance.

SAMPLE 2 — COMPLIANCE CONTROL NARRATIVE

5 Control Narrative: Privileged Access Governance

5.1 Control Objective

The organization maintains strict control over privileged system access to prevent unauthorized activity, support operational reliability, and meet audit and regulatory compliance obligations.

Control Description (Narrative Format)

Privileged access is treated as a governance-controlled function, not a routine IT task. All administrative accounts are provisioned only after documented business justification, formal approval, and compliance validation.

Requests are routed through an ITSM-controlled workflow to ensure traceability. Access is granted using least privilege enforcement and is uniquely assigned to prevent shared credential risk.

System activity is continuously logged, monitored, and retained as evidence. Quarterly access reviews ensure privileges remain aligned with job role requirements and are promptly revoked when no longer necessary.

5.2 Evidence and Audit Defensibility

Auditors can validate compliance through:

- Ticketed approval workflows
- Privileged access registries
- Logging retention reports
- Quarterly certification reviews

5.3 Operational Impact

This control ensures governance-level accountability, reduces cyber and reliability exposure, and strengthens institutional resilience under regulatory scrutiny.

SAMPLE 3 — KNOWLEDGE BASE ARTICLE (SERVICE DESK STYLE)

6 KB-112: How to Request Elevated System Access

6.1 Overview

This article provides instructions for requesting elevated or administrative access to enterprise systems.

6.2 When to Use

Submit this request when:

- You require temporary admin rights for implementation work
- You are assigned to a regulated operational support role
- A privileged task cannot be completed under standard access

6.3 Steps to Request Access

- Log into the ServiceNow Portal
- Navigate to: **Access Requests → Privileged Access**
- Complete required fields:

1. System name
2. Role requested
3. Business justification
4. Start and end date (if temporary)
5. Submit request for approval

6.4 What Happens Next

- Your System Owner reviews the request
- Compliance confirms policy alignment
- IT Security provisions access if approved

6.5 Important Notes

- Privileged access is monitored and logged
- Shared accounts are not permitted
- Access is subject to quarterly review

6.6 Support

If you need help completing the form, contact the Service Desk or your Compliance Lead.

PAGE LEFT
INTENTIONALLY
BLANK

LISA BROWN

Tech Writing Portfolio

Style Samples v2026.1

---

lbanet2go@yahoo.com 484.891.1068