

Cyber Security Resilience

A Complete Guide - 2019 Edition



PRACTICAL TOOLS FOR SELF-ASSESSMENT

Diagnose projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices

Implement evidence-based best practice strategies aligned with overall goals

Integrate recent advances and process design strategies into practice according to best practice guidelines

Use the Self-Assessment tool Scorecard and develop a clear picture of which areas need attention

The 2019 Edition

Cyber Security Resilience Complete Self-Assessment Guide

The guidance in this Self-Assessment is based on Cyber Security Resilience best practices and standards in business process architecture, design and quality management. The guidance is also based on the professional judgment of the individual collaborators listed in the Acknowledgments.

Notice of rights

You are licensed to use the Self-Assessment contents in your presentations and materials for internal use and customers without asking us - we are here to help.

All rights reserved for the book itself: this book may not be reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

The information in this book is distributed on an "As Is" basis without warranty. While every precaution has been taken in the preparation of the book, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the products described in it.

Trademarks

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.

Copyright © by The Art of Service
<http://theartofservice.com>
service@theartofservice.com



Table of Contents

About The Art of Service	8
Acknowledgments	9
Included Resources - how to access	10
Your feedback is invaluable to us	12
Purpose of this Self-Assessment	12
How to use the Self-Assessment	13
Cyber Security Resilience Scorecard Example	15
Cyber Security Resilience Scorecard	16
BEGINNING OF THE SELF-ASSESSMENT:	17
CRITERION #1: RECOGNIZE	18
CRITERION #2: DEFINE:	27
CRITERION #3: MEASURE:	44
CRITERION #4: ANALYZE:	64
CRITERION #5: IMPROVE:	79
CRITERION #6: CONTROL:	93
CRITERION #7: SUSTAIN:	106
Cyber Security Resilience and Managing Projects, Criteria for Project Managers:	135
1.0 Initiating Process Group: Cyber Security Resilience	136
1.1 Project Charter: Cyber Security Resilience	138
1.2 Stakeholder Register: Cyber Security Resilience	140

1.3 Stakeholder Analysis Matrix: Cyber Security Resilience	141
2.0 Planning Process Group: Cyber Security Resilience	143
2.1 Project Management Plan: Cyber Security Resilience	145
2.2 Scope Management Plan: Cyber Security Resilience	147
2.3 Requirements Management Plan: Cyber Security Resilience	149
2.4 Requirements Documentation: Cyber Security Resilience	151
2.5 Requirements Traceability Matrix: Cyber Security Resilience	153
2.6 Project Scope Statement: Cyber Security Resilience	155
2.7 Assumption and Constraint Log: Cyber Security Resilience	157
2.8 Work Breakdown Structure: Cyber Security Resilience	159
2.9 WBS Dictionary: Cyber Security Resilience	161
2.10 Schedule Management Plan: Cyber Security Resilience	164
2.11 Activity List: Cyber Security Resilience	166
2.12 Activity Attributes: Cyber Security Resilience	168
2.13 Milestone List: Cyber Security Resilience	170
2.14 Network Diagram: Cyber Security Resilience	172

2.15 Activity Resource Requirements: Cyber Security Resilience	174
2.16 Resource Breakdown Structure: Cyber Security Resilience	175
2.17 Activity Duration Estimates: Cyber Security Resilience	177
2.18 Duration Estimating Worksheet: Cyber Security Resilience	180
2.19 Project Schedule: Cyber Security Resilience	182
2.20 Cost Management Plan: Cyber Security Resilience	184
2.21 Activity Cost Estimates: Cyber Security Resilience	186
2.22 Cost Estimating Worksheet: Cyber Security Resilience	188
2.23 Cost Baseline: Cyber Security Resilience	190
2.24 Quality Management Plan: Cyber Security Resilience	192
2.25 Quality Metrics: Cyber Security Resilience	194
2.26 Process Improvement Plan: Cyber Security Resilience	196
2.27 Responsibility Assignment Matrix: Cyber Security Resilience	198
2.28 Roles and Responsibilities: Cyber Security Resilience	200
2.29 Human Resource Management Plan: Cyber Security Resilience	202

2.30 Communications Management Plan: Cyber Security Resilience	204
2.31 Risk Management Plan: Cyber Security Resilience	206
2.32 Risk Register: Cyber Security Resilience	208
2.33 Probability and Impact Assessment: Cyber Security Resilience	210
2.34 Probability and Impact Matrix: Cyber Security Resilience	212
2.35 Risk Data Sheet: Cyber Security Resilience	214
2.36 Procurement Management Plan: Cyber Security Resilience	216
2.37 Source Selection Criteria: Cyber Security Resilience	218
2.38 Stakeholder Management Plan: Cyber Security Resilience	220
2.39 Change Management Plan: Cyber Security Resilience	222
3.0 Executing Process Group: Cyber Security Resilience	224
3.1 Team Member Status Report: Cyber Security Resilience	226
3.2 Change Request: Cyber Security Resilience	228
3.3 Change Log: Cyber Security Resilience	230
3.4 Decision Log: Cyber Security Resilience	232
3.5 Quality Audit: Cyber Security Resilience	234

3.6 Team Directory: Cyber Security Resilience	237
3.7 Team Operating Agreement: Cyber Security Resilience	239
3.8 Team Performance Assessment: Cyber Security Resilience	241
3.9 Team Member Performance Assessment: Cyber Security Resilience	243
3.10 Issue Log: Cyber Security Resilience	245
4.0 Monitoring and Controlling Process Group: Cyber Security Resilience	247
4.1 Project Performance Report: Cyber Security Resilience	249
4.2 Variance Analysis: Cyber Security Resilience	251
4.3 Earned Value Status: Cyber Security Resilience	253
4.4 Risk Audit: Cyber Security Resilience	255
4.5 Contractor Status Report: Cyber Security Resilience	257
4.6 Formal Acceptance: Cyber Security Resilience	259
5.0 Closing Process Group: Cyber Security Resilience	261
5.1 Procurement Audit: Cyber Security Resilience	263
5.2 Contract Close-Out: Cyber Security Resilience	266
5.3 Project or Phase Close-Out: Cyber Security Resilience	268
5.4 Lessons Learned: Cyber Security Resilience	270

Is the operating system up to date?
confidentiality of your information?
handled?

Defining, designing, creating, and i
able role... In EVERY group, comp

Unless you are talking a one-time,
and implemented by humans, AI, o
enough perspective to ask the right
'What are we really trying to accomplish here? And is there a different way to look at it?'

This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-) President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Cyber Security Resilience investments work better.

This Cyber Security Resilience All-Inclusive Self-Assessment enables You to be that person.

All the tools you need to an in-depth Cyber Security Resilience Self-Assessment. Featuring 977 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Cyber Security Resilience improvements can be made.

In using the questions you will be better able to:

- diagnose Cyber Security Resilience projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices
- implement evidence-based best practice strategies aligned with overall goals
- integrate recent advances in Cyber Security Resilience and process design strategies into practice according to best practice guidelines

Using a Self-Assessment tool known as the Cyber Security Resilience Scorecard, you will develop a clear picture of which Cyber Security Resilience areas need attention.

Your purchase includes access details to the Cyber Security Resilience self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. You will receive the following contents with New and Updated specific criteria:

- The latest quick edition of the book in PDF
- The latest complete edition of the book in PDF, which criteria correspond to the criteria in...
- The Self-Assessment Excel Dashboard
- Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation
- In-depth and specific Cyber Security Resilience Checklists
- Project management checklists and templates to assist with implementation

INCLUDES LIFETIME SELF ASSESSMENT UPDATES

Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

Biblioteka Główna

Akademii Sztuki Wojennej

26630/III (CB)



03-026630-000-0

-JY.

ISBN 9780655801320

9 780655 801320