Cyber Security Risk Management

COMPLETE SELF-ASSESSMENT GUIDE

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 index-graph and develop a clear picture of which areas need attention

The Art of Service

Disclaimer

The guidance in this Self-Assessment is based on Cyber Security Risk Management 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 permitted 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 he 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.

http://theartofservice.com
service@theartofservice.com

Contents

About The Art of Service 3
Acknowledgments 4
Included Resources - how to access 5
Your feedback is invaluable to us 6
Purpose of this Self-Assessment 7
How to use the Self-Assessment 8
Cyber Security Risk Management
Index Example 10
Cyber Security Risk Management
Index 11
CRITERION #1: RECOGNIZE 12
CRITERION #2: DEFINE: 16
CRITERION #3: MEASURE: 27
CRITERION #4: ANALYZE: 37
CRITERION #5: IMPROVE: 42
CRITERION #6: CONTROL: 51
CRITERION #7: SUSTAIN: 59
Index 61

How do we keep improving Cyb [illegible] schedule according to the plan? What [illegible] ere any constraints known that bear [illegible] n addressing them? Does Cyber Se [illegible] ility and quality improvement?

Defining, designing, creating, ar [illegible] ctive is the most valuable role… In E [illegible]

Unless you are talking a one-tim [illegible] process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?'

For more than twenty years, The Art of Service's Self-Assessments empower people who can do just that - whether their title is marketer, entrepreneur, manager, salesperson, consultant, business process manager, executive assistant, IT Manager, CxO etc... - they are the people who rule the future. They are people who watch the process as it happens, and ask the right questions to make the process work better.

This book is for managers, advisors, consultants, specialists, professionals and anyone interested in Cyber Security Risk Management assessment.

Featuring 372 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 Risk Management improvements can be made.

In using the questions you will be better able to:

- diagnose Cyber Security Risk Management 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 Risk Management and process design strategies into practice according to best practice guidelines

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

Included with your purchase of the book is the Cyber Security Risk Management Self-Assessment downloadable resource, containing all questions and Self-Assessment areas of this book. This enables ease of (re-)use and enables you to import the questions in your preferred management tool. Access instructions can be found in the book.

You are free to use the Self-Assessment contents in your presentations and materials for customers without asking us - we are here to help. This Self-Assessment has been approved by The Art of Service as part of a lifelong learning and Self-Assessment program and as a component of maintenance of certification. Optional other Self-Assessments are available. For more information, visit http://theartofservice.com

ISBN 9781489142412

9 781489 142412