

Cyber Security Incident Response

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 Art of Service

Cyber Security Incident Response Complete Self-Assessment Guide

The guidance in this Self-Assessment is based on Cyber Security Incident Response 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 Incident Response	15
Scorecard Example	15
Cyber Security Incident Response	
Scorecard	16
BEGINNING OF THE	
SELF-ASSESSMENT:	17
CRITERION #1: RECOGNIZE	18
CRITERION #2: DEFINE:	29
CRITERION #3: MEASURE:	45
CRITERION #4: ANALYZE:	59
CRITERION #5: IMPROVE:	71
CRITERION #6: CONTROL:	85
CRITERION #7: SUSTAIN:	98
Cyber Security Incident Response and Managing Projects, Criteria for Project Managers:	135
1.0 Initiating Process Group: Cyber Security Incident Response	136
1.1 Project Charter: Cyber Security Incident Response	138

1.2 Stakeholder Register: Cyber Security Incident Response	140
1.3 Stakeholder Analysis Matrix: Cyber Security Incident Response	141
2.0 Planning Process Group: Cyber Security Incident Response	143
2.1 Project Management Plan: Cyber Security Incident Response	145
2.2 Scope Management Plan: Cyber Security Incident Response	147
2.3 Requirements Management Plan: Cyber Security Incident Response	149
2.4 Requirements Documentation: Cyber Security Incident Response	151
2.5 Requirements Traceability Matrix: Cyber Security Incident Response	153
2.6 Project Scope Statement: Cyber Security Incident Response	155
2.7 Assumption and Constraint Log: Cyber Security Incident Response	157
2.8 Work Breakdown Structure: Cyber Security Incident Response	160
2.9 WBS Dictionary: Cyber Security Incident Response	162
2.10 Schedule Management Plan: Cyber Security Incident Response	164

2.11 Activity List: Cyber Security Incident Response	166
2.12 Activity Attributes: Cyber Security Incident Response	168
2.13 Milestone List: Cyber Security Incident Response	170
2.14 Network Diagram: Cyber Security Incident Response	172
2.15 Activity Resource Requirements: Cyber Security Incident Response	174
2.16 Resource Breakdown Structure: Cyber Security Incident Response	176
2.17 Activity Duration Estimates: Cyber Security Incident Response	178
2.18 Duration Estimating Worksheet: Cyber Security Incident Response	180
2.19 Project Schedule: Cyber Security Incident Response	182
2.20 Cost Management Plan: Cyber Security Incident Response	184
2.21 Activity Cost Estimates: Cyber Security Incident Response	186
2.22 Cost Estimating Worksheet: Cyber Security Incident Response	188
2.23 Cost Baseline: Cyber Security Incident Response	190
2.24 Quality Management Plan: Cyber Security Incident Response	192

2.25 Quality Metrics: Cyber Security Incident Response	194
2.26 Process Improvement Plan: Cyber Security Incident Response	196
2.27 Responsibility Assignment Matrix: Cyber Security Incident Response	198
2.28 Roles and Responsibilities: Cyber Security Incident Response	200
2.29 Human Resource Management Plan: Cyber Security Incident Response	202
2.30 Communications Management Plan: Cyber Security Incident Response	204
2.31 Risk Management Plan: Cyber Security Incident Response	206
2.32 Risk Register: Cyber Security Incident Response	208
2.33 Probability and Impact Assessment: Cyber Security Incident Response	210
2.34 Probability and Impact Matrix: Cyber Security Incident Response	212
2.35 Risk Data Sheet: Cyber Security Incident Response	214
2.36 Procurement Management Plan: Cyber Security Incident Response	216
2.37 Source Selection Criteria: Cyber Security Incident Response	218
2.38 Stakeholder Management Plan: Cyber Security Incident Response	220

2.39 Change Management Plan: Cyber Security Incident Response	222
3.0 Executing Process Group: Cyber Security Incident Response	224
3.1 Team Member Status Report: Cyber Security Incident Response	226
3.2 Change Request: Cyber Security Incident Response	228
3.3 Change Log: Cyber Security Incident Response	230
3.4 Decision Log: Cyber Security Incident Response	232
3.5 Quality Audit: Cyber Security Incident Response	234
3.6 Team Directory: Cyber Security Incident Response	237
3.7 Team Operating Agreement: Cyber Security Incident Response	239
3.8 Team Performance Assessment: Cyber Security Incident Response	241
3.9 Team Member Performance Assessment: Cyber Security Incident Response	243
3.10 Issue Log: Cyber Security Incident Response	245
4.0 Monitoring and Controlling Process Group: Cyber Security Incident Response	247
4.1 Project Performance Report: Cyber Security Incident Response	249
4.2 Variance Analysis: Cyber Security Incident Response	251

4.3 Earned Value Status: Cyber Security Incident Response	253
4.4 Risk Audit: Cyber Security Incident Response	255
4.5 Contractor Status Report: Cyber Security Incident Response	257
4.6 Formal Acceptance: Cyber Security Incident Response	259
5.0 Closing Process Group: Cyber Security Incident Response	261
5.1 Procurement Audit: Cyber Security Incident Response	263
5.2 Contract Close-Out: Cyber Security Incident Response	265
5.3 Project or Phase Close-Out: Cyber Security Incident Response	267
5.4 Lessons Learned: Cyber Security Incident Response	269
Index	272

Biblioteka Główna
Akademii Sztuki Wojennej

26629/III (CB)



03-026629-000-0

ri
nt
je-

What have you done? What is the
What arrangements are in place to

This premium Cyber Security Incid
Response domain auditor by reve
Incident Response challenge.

How do I reduce the effort in the C
ensure that plans of action include
Response outcome is in place? How
curity Incident Response costs are low? How can I deliver tailored Cyber Security Incident Response advice instantly
with structured going-forward plans?

There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk.
Blokdyk ensures all Cyber Security Incident Response essentials are covered, from every angle: the Cyber Security Inci
dent Response self-assessment shows succinctly and clearly that what needs to be clarified to organize the required
activities and processes so that Cyber Security Incident Response outcomes are achieved.

Contains extensive criteria grounded in past and current successful projects and activities by experienced Cyber Secu
rity Incident Response practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides
its superior value to you in knowing how to ensure the outcome of any efforts in Cyber Security Incident Response are
maximized with professional results.

Your purchase includes access details to the Cyber Security Incident Response self-assessment dashboard download
which gives you your dynamically prioritized projects-ready tool and shows you exactly what to do next. Your exclusive
instant access details can be found in your book. 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 Incident Response 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.

ISBN 9780655518471

9 780655 518471