FRAMEWORKS & SELF-ASSESSMENTS

INTRODUCTION

Companies have all set specific goals and follow-through mechanisms to produce intended results, with consideration for ever-changing social, regulatory and market environment parameters. Millions of them base their operational processes thereby around worldwide accepted norms and standards. Over time however, the constantly changing environment will affect some of these operational processes results. To investigate suspected deviations and to check that just enough of the right kinds of risks are taken to effectively pursue intended goals, it is recommended to do a self-assessment (also called compliance testing) to produce a dashboard as a basis for corrective action. Below is an example of the kind of dashboard used for checking EU General Data Protection Regulation compliance using a Privacy Control Framework (PCF) resulting from self-assessment work. The focus is on the rightmost column of below dashboard, Risk Action. Instructions on how to build the input for this dashboard follow further.

GDPR – Data lifecycle assessment dashboard by Risk Action

Ref.	Name	#Tests	Importance	Risk Assess	Risk Score	CO Assess	CO Score	Risk Action
Controls & Risks by Risk Action								
CFR01	Privacy Statement must have requirements for Choice and Consent	0	Moderate	Moderate	2	Adequate Controls	2	Tolerate
PST02	Privacy Statement must have requirements for Notice	0	High	High	3	Good Controls	3	Tolerate
Risk Action	**CO Count**	**AVG. CO Score**	**Set Risk Count**	**AVG. Risk Score**				
Tolerate	2	2,50	2	2,50				
PST01	Privacy Statement scope	0	High	High	3	Poor Controls	1	Treat
Risk Action	**CO Count**	**AVG. CO Score**	**Set Risk Count**	**AVG. Risk Score**				
Treat	1	1,00	1	3,00				

TIMING

Executing a self-assessment to produce the resulting dashboard will largely depend on the complexity of the framework you want to assess against and the number of suspected weak spots you want to investigate. Assessment templates are currently available for Information Technology, Information Security and Privacy Regulations. These all include all hierarchical sections of the framework, which you can easily scope in or out, in scope being the default. In addition, you can narrow your work by just assessing your suspected pain points at the Control Objectives level. Empty scores will not influence the resulting dashboard. If you are familiar with the operational environment and the framework being assessed, and, you are not depending on answers to be provided by colleagues, a Control Objective can be assessed within minutes. Remember that you want to confirm suspected weak spots quickly, but that is depending on assessing the right Control Objectives, i.e. you might be overlooking things. If in doubt we can provide you with a second opinion.

ASSESMENT FRAMEWORK CONSTRUCTIONS	Example PRIVACY CONTROL FRAMEWORK
Standard specific hierarchy Section(s)	Section 2 – Choice and Consent
Control Objective(s) or CO(s) for this Section	Control Objective - CFR - Consent framework
Control(s) for each Control Objective	Control CFR02 Subject consent processing
Test(s) for each Control (where available)	Test DPP1.1 Processing details communication

SUPPORT

We are available to coach you through the exercise. In addition, we can provide templates in function of your specific needs. If for example, you do not want to investigate the Management System sections of Information Security or Privacy Compliance, we can reduce the assessment template size drastically.

SELF-ASSESSMENT GUIDANCE FOR - CobiT for GDPR & Board Risk Control by ISACA

Disclaimer: Your rights and obligations

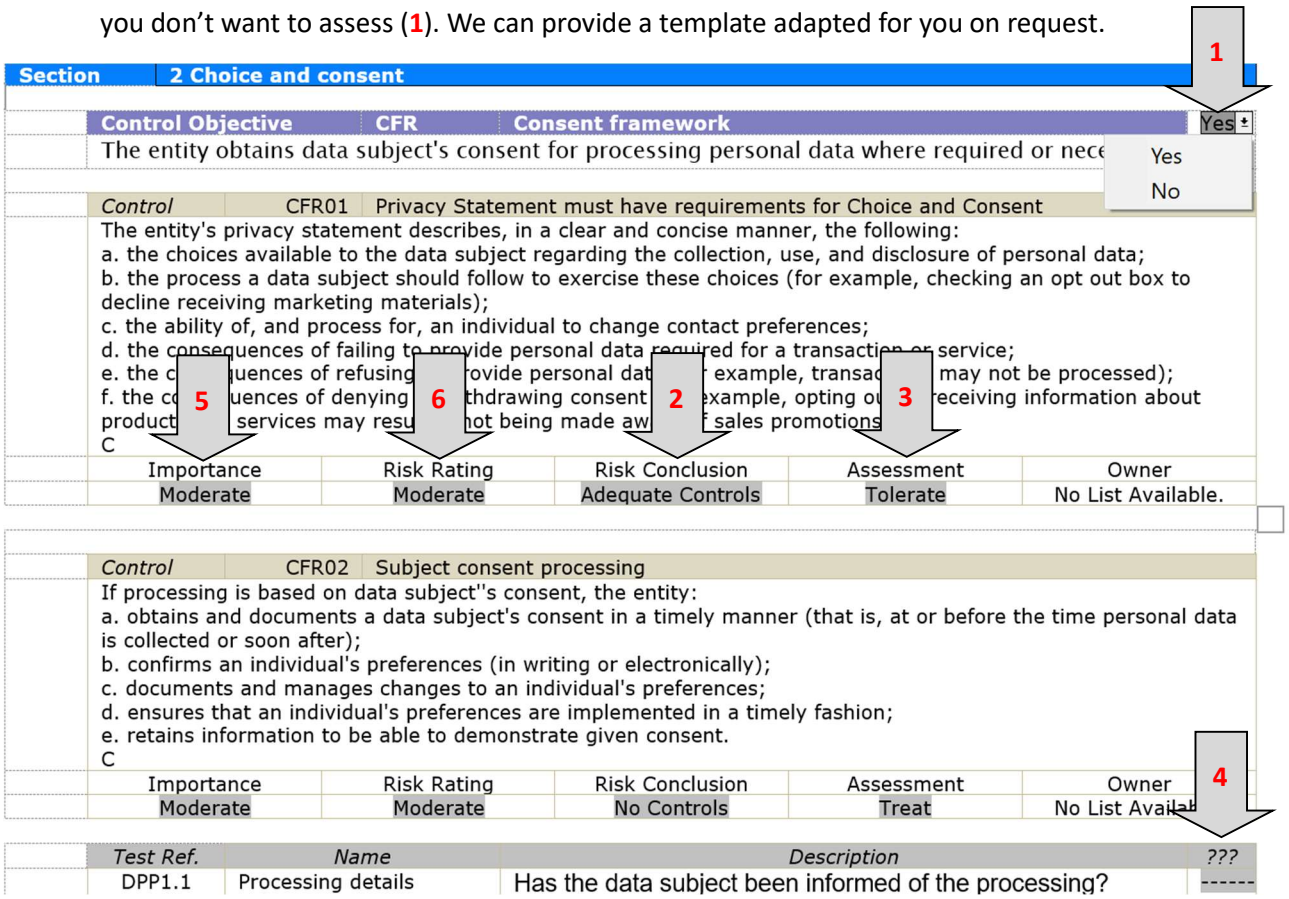
1) Observe the rights and reservations of the framework publisher.
2) The Self-Assessment document is produced with CoBIT 4.0 Management and Methodware Pathfinder software under trademarks of Methodware Limited New Zealand. This software is based on CobiT®4.0, copyright © 2005 by the IT Governance Institute, and is used with permission. Methodware is not affiliated with the Information Systems Audit and Control Foundation or the IT Governance Institute.
3) No part of the Self-Assessment document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including but not limited to photocopying, without prior written permission from QPMC. Copying or duplicating the documentation or any part thereof is a violation of the law.

Step 1: Prepare your assessment

- Decide what concerns (suspected risks) you would like to evaluate within the framework and what you certainly do not want to cover in your scope. Limit your first scope choice to the top 3 suspected Control Objectives. This will help you understand the assessment cycle.
- Note that the resulting dashboard will only reflect correct information if you ensure that all Controls below each Control Objective within scope are evaluated.

Step 2: Execute your assessment using the self-assessment form

- By default, all Control Objectives are within scope, so select no in the dropdown selector for those you don't want to assess (1). We can provide a template adapted for you on request.



- Next assess all Controls below the scoped in Control Objectives. If you judge a particular Control to be working OK, you can give a neutral risk assessment by selecting a Risk Conclusion of "Adequate

Controls" (2) and a Control Assessment of "Tolerate" (3). Below the Controls, Tests, where available, are intended to help you judge the effectiveness of each Control. The Test dropdown in the "???" list (4) will not influence the dashboard scoring results. You can either use it to mark test compliance (Satisfactory or Unsatisfactory) or for timing purposes (Pending or Planned). In some cases, tests might not be available as you'd expect them for your environment. Alternative tests from field experience will gradually be added if they are useful in other environments, so your input or feedback/contribution will be highly appreciated.

- Next refine your first evaluation considering the business aspects. You yourself or, preferably in concertation with competent business process owners, can decide a judgement value for your business environments' importance from the Importance List (5), together with a belly-based Risk Rating from the Risk Rating List (6) for each Control. Next revise the Risk Conclusion action from the Risk Conclusion List (2), based on looking into the risk factors in the assets you use to run your day-to-day business activity. Adjust the overall Assessment (3) in function of the revised Controls effectiveness, providing a more accurate risk exposure conclusion.
- Next document your findings and the action(s) you judge necessary to mitigate the exposure.

Step 3: Follow up and Conclusions

- Complete your assessment step by step, leaving comments and suggestions as per the comments & suggestions topic on the next page. NEVER CHANGE THE RTF format when saving the assessment file.
- You may want to embed the resulting assessment form file in a password protected archive to keep the information confidential.

Step 4: Dashboard production & Clarifications

- QPMC will return the resulting dashboard to you with basic comments and remarks that we can further discuss if clarification is needed.
- Different dashboards are available grouped by Control Importance, Control Assessment, Risk Rating or Risk Conclusion. It is recommended to work based on the resulting Risk Conclusions to prioritize your action plans.

Lists & Scores: Reflecting the status lists and assessment criteria with respective weight values where applicable

(1) Control Objective scope (No Label): Yes/Include, No/Exclude from Dashboard calculations

(2) Control Effectiveness Conclusion (Label "Risk Conclusion"): -Not Set-/0, No Controls/0, Poor Controls/1, Adequate Controls/2, Good Controls/3, Excellent Controls/4

(3) Control Risk Conclusion (Label "Assessment"): -Not Set-, Tolerate, Treat, Transfer, Terminate

(4) Test Status (Label "????"): Pending, Planned, Satisfactory, Unsatisfactory

(5) Control Importance (Label "Importance"): -Not Set-/0, Low/1, Moderate/2, High3

(6) Control Risk Rating (Label "Risk Rating"): -Not Set-/0, Low/1, Moderate/2, High/3

COMMENTS & SUGGESTIONS FOR - CobiT for GDPR & Board Risk Control by ISACA

Any comment for improvement is welcome at training@qpmc.com.

Any suggested tests are very welcome and will be shared with the other contributors for review and feedback at above e-mail address.