A Framework for Assessing 20 Critical Controls Using ISO 15504 and COBIT 5 Process Assessment Model (PAM)

GIAC (GCCC) Gold Certification

Author: Muzamil Riffat, muzamil@hotmail.com
Advisor: Stephen Northcutt

Accepted: April 7, 2015

Abstract

The 20 critical controls, maintained by the Council on CyberSecurity, present a prioritized road map for organizations to enhance their information security posture. However, an initial review that serves as a "baseline" must first be performed to know the current information security posture and to ascertain the effort required to implement the critical controls. Furthermore, assessments or audits should be performed periodically to gauge the continual improvement in information security as well as to what extent the critical controls have been implemented. This paper presents a unified and repeatable framework that could be used for the initial gap analysis as well as to measure the continual enhancements in implementation of the critical controls. The concepts presented in this paper draw heavily from the contents contained in "ISO/IEC 15504 Information technology — Process assessment" standard and COBIT5 Process Assessment Model (PAM). The information presented in ISO 15504 and COBIT 5 PAM is adapted for the assessment of critical controls. A unified approach in assessing the implementation status of each critical control as well as the sub-controls is presented based on an incremental measuring scale. The other peripheral elements of the assessment such as the details of assessment process (planning, initiation, fieldwork reporting), assessor qualifications, and competency are also detailed out resulting in a comprehensive framework for assessing the 20 critical controls.

1. Introduction

In order to gain competitive advantage and efficiency, Information Technology (IT) is used in almost all aspects of business today. Working with IT to build and implement Information Systems (IS) is certainly not straight forward, and failures often darken the blue skies predicted by IT suppliers and vendors (Conboy 2010, Dwivedi et al. 2013). Once the information systems have been developed, securing them is an even more difficult task. Literature on information security risk management based on international standards is scarce (Al-Ahmad & Mohammad, 2013) and there are moments in IT management when a practitioner may feel like the Scarecrow in The Wizard of Oz who so desperately wants a brain (Suer, 2013). Most organizations obtain a false sense of security by investing in the latest tools. Although tools and technologies are an integral part of an organization’s information security plans, it is argued that they alone are not sufficient to address information security problems (Herath & Rao, 2009). With all these challenges in mind, “The 20 Critical Controls” present a prioritized list of technical controls that organizations can consider implementing and auditing against in order to assess their security posture.

As a best practice, the first step is to assess the existing process capability level/organizational maturity level (Wysocki, 2004). The methodology used for this initial review and for future assessments should be repeatable so that consistent results are derived from the assessments. The assessment can be used internally for reporting to the management and to establish a target for improvement based on the business requirements, as appropriate. Another goal of the methodological assessment is to reduce the degree of subjectivity in order to present the findings and to document the action plans for areas of improvement. In addition to delivering immediate added market value from process capability assessment results in their own right (more reliable process capability assessment results provide a superior basis from which process improvement plans can be developed), such improvements can also provide the basis for the establishment of broader maturity assessments that may be of value to certain enterprises and their customers, should such a demand arise (Shanahan, 2011).

There are other critical success factors that must be considered in order to realize the expected benefits. The most important of such factors is the management support and sponsorship for the assessment. Having the adequate management support ensures that resources and competencies are made available for performing the assessment and improvement plans are effectively implemented in a timely manner. Furthermore, the scope and constraints should be clearly identified as well. For example, it should be clearly stated which geographical locations and offices fall under the review.

Finally, if the results of the assessment are compared with results from other organizations in order to compare security posture, appropriate consideration should be given without relying solely on the numerical results of the assessment. Information security is a broad field, and the critical controls only present a subset of technical controls that should be implemented. The data compromise could also happen due to non-technical controls that are embedded in the day-to-day operations. Therefore, the assessment of critical controls, and improvement plans thereof, should only be considered a way of enhancing the security posture through implementation of technical controls.

2. Re-examining the terminology

The official documentation refers the 20 IT areas as critical "controls." However, the definition of "control" might vary from person to person. The Institute of Internal Auditors (IIA), the recognized authority for internal auditing, defines control as "Any action taken by management, the board and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved." It is clear from the definition that the focus of the control is narrow and on a limited set of activities. It can be argued that a better term would be to use "process," i.e. "20 Critical Processes," instead of "20 Critical Controls." A process is characterized by an input, a set of analysis activities, and an output. The monitoring mechanisms or Key Performance Indicators (KPIs) are also more associated with the term "process" rather than with "control." Similarly, the evaluation tests as mentioned in the official document of critical controls could be considered to be more applicable if the "process" terminology is used. Furthermore, the SANS course for

20 Critical Controls refers to the use of Unified Model Language (UML) as "… to better visualize the systems and controls that interact with each other within each Critical Control." However, in the definition of UML on its official page, the reference is made to "process." The official definition reads "UML is Object Management Group's most-used specification, and the way the world models not only application structure, behavior, and architecture, but also business process and data structure" (http://www.uml.org). The official body of Critical Controls should re-examine the terminology. If it is determined that "control" is the right term, appropriate references, declarations, and explanations should be made to substantiate such a decision.

To be consistent with the terminology used in the official documentation, the terms "controls" and "processes" are used interchangeably throughout the rest of this document.

3. Assessment Methodology

3.1. Measurement Framework

ISO 15504 defines specific rating criteria for evaluation. According to the criteria mentioned in ISO 15504 standard, all controls should be assessed on a scale of 0 to 5 (0 as the lowest capability rating and 5 as the highest capability rating).

3.1.1. Sub-Controls Assessment

There are currently 182 sub-controls within the 20 critical controls. All 182 controls can be assessed at three levels depending upon the implementation status, and numeric score can be assigned to them accordingly. The table below indicates the rating and suggested numeric score for each rating.

Rating Description	Numeric Score
Fully Addressed	1
Partially Addressed	0.5
Not Addressed	0

Figure 1: Sub-Controls Rating Scheme

Once the assessment of all controls is done, a table summarizing the overall implementation status can be prepared as shown below.

Control #	Description	Total Sub-Controls	Implementation Equivalence
CSC 1	Inventory of Authorized and Unauthorized Devices	7	3.5
CSC 2	Inventory of Authorized and Unauthorized Software	9	6
…	…..	…	…
…	…..	…	…
CSC 20	Penetration Tests and Red Team Exercises	8	6
Total		182	nnn

Figure 2: Summarized Table Showing Implementation Status

In Figure 2, the implementation equivalence (last column) is calculated by first assigning each sub-control a numeric score of 0, 0.5, or 1 depending upon the implementation status as mentioned in Figure 1. The numeric scores for all sub-controls for each control are then added to come up with the overall implementation equivalence.

3.1.2. Capability Levels

As defined in ISO 15504-2 and applied in COBIT 5 PAM, there are six maturity/capability levels that can be used to depict the status of each critical control. These maturity levels are based on an incremental scale from 0 to 5. The first level "Level 0: Incomplete" indicates that process/controls are not implemented or are failing to achieve the purpose. There is little to no evidence of any systematic achievement of the purpose. The next level, "Level 1: Performed" shows that implemented process/controls achieve their purpose. "Level 2: Managed" specifies that the process is now implemented in a managed fashion (planned, monitored, and adjusted), and its work products are appropriately established, controlled, and maintained. "Level 3: Established" means that managed process is now implemented as a defined process that is capable of achieving its process outcomes. The "Level 4: Predictable" indicates that the established process now operates within defined limits to achieve its process outcomes as a measured and controlled process. The last level, "Level 5: Optimizing" demonstrates that the predictable process is continuously improved to meet relevant, current, and projected business goals, incorporating innovation and optimization. The figure below depicts the capability level in the graphical format.

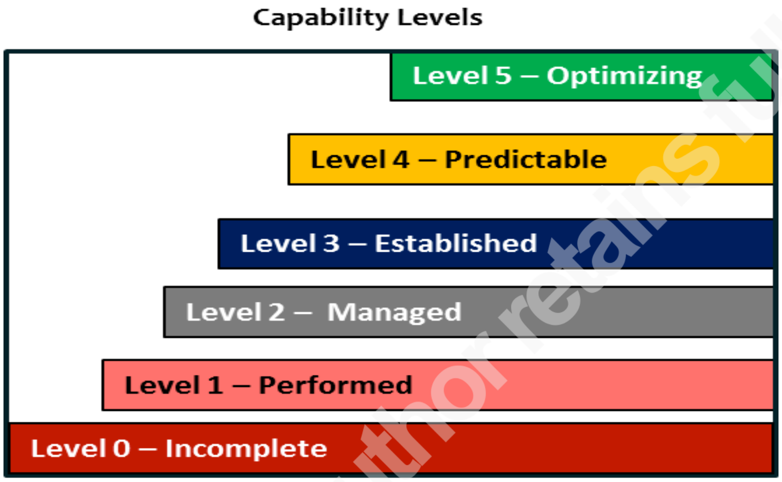


Figure 3: Capability Levels Based Upon ISO 15504-2

It is important to appreciate the fact that not all controls or processes might require the highest level (Optimizing) capability or maturity. Depending upon the cost-benefit analysis and other related factors, management should set a target for each process/control and perform the assessment against the agreed upon target.

In order to evaluate the maturity of each control or process, the following formula can be used (source: author):

$$\left({SumOfNumericRatingForSubControls}\Big/{TotalSubControls} \right) * 5$$

3.1.3. Overall Summary of Assessment

Once the above mentioned formula has been applied to all controls, a summary graph can be prepared that shows the overall maturity or capability status of each control. An illustrative graph for a government organization in the Middle East is shown below for reference purposes:

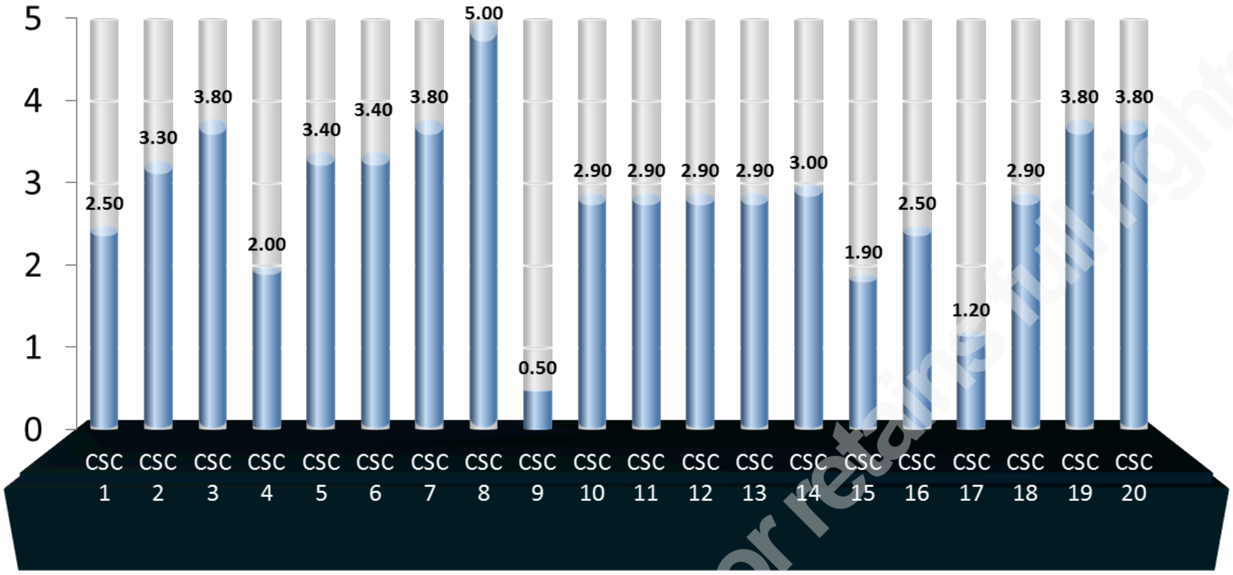


Figure 4: Sample Graph Showing Summary of Ratings for each Control
CSC refers to Critical Security Control; # refers to the number of the security control

Management/stakeholders involved in the assessment might also be interested in getting information about the controls implementation status as per the category of each control. The following illustrative graph for a government organization in the Middle East can be used to demonstrate this information (source: author).

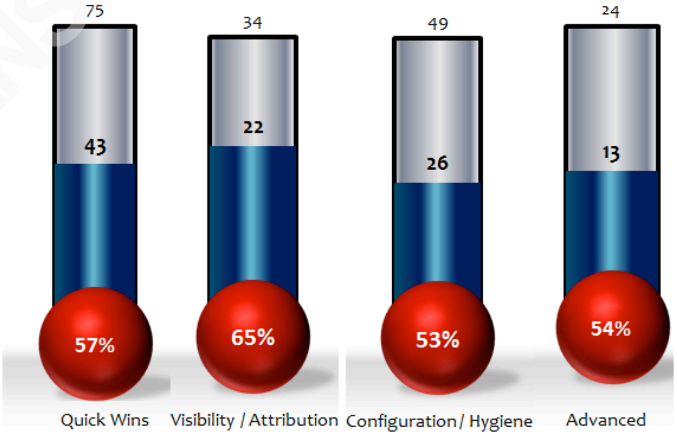


Figure 5: Sample Graph Showing Summary by Controls Category

Muzamil Riffat, muzamil@hotmail.com

3.1.4. Implementation/Improvement Roadmap

The gaps identified as a result of the assessment can be remediated in several ways. Since the critical controls present a prioritized list, management might consider the implementation of controls in numerical sequence i.e. first implementing control 1, then control 2, and so on and so forth.

Another method might be to first focus on "*Quick Wins"* category. According to the official Critical Controls document, "the intent of identifying Quick Win areas is to highlight where security can be improved rapidly …without major procedural, architectural or technical changes". It is also noteworthy that for each control, the impact on attack mitigation has already been identified. Therefore, the combination of these two pieces of information (controls category and impact on attack mitigation) can be used to prepare an implementation roadmap whereby all *Quick Win* areas would be focused in short-term (e.g. 3 to 6 months) and implementation of all other controls areas would be done in long term (6 months to 18 months). Assuming there are 104 out of 182 sub-controls (with details below) that are identified for implementation, the following illustrative graph can be used to prepare the implementation roadmap (source: author).

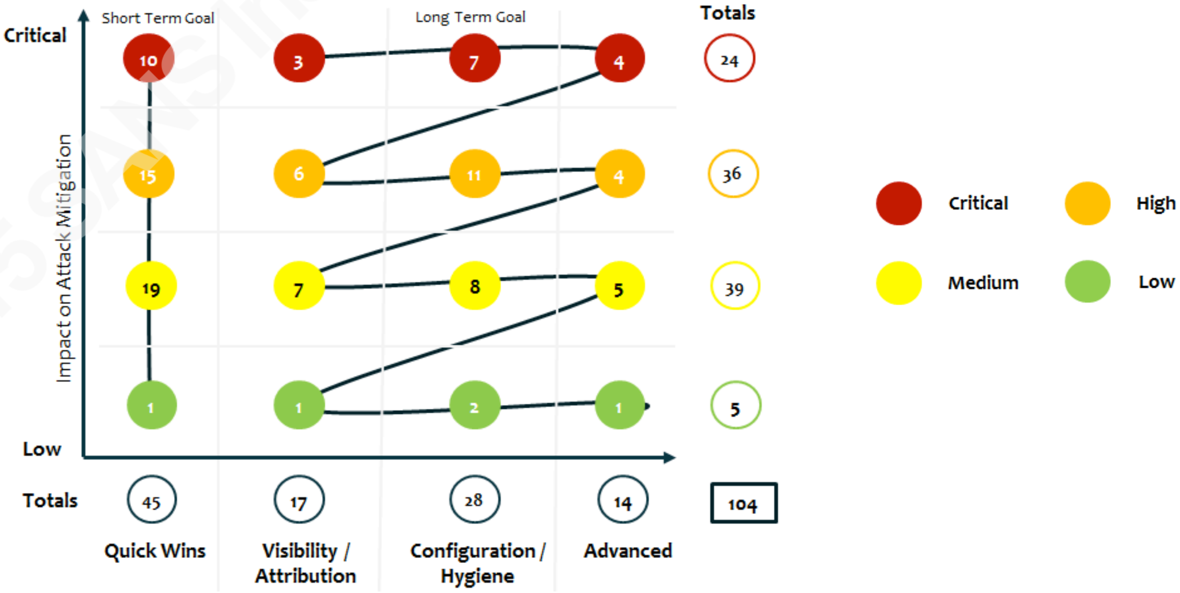


Figure 6: Sample Improvement Plan

Muzamil Riffat, muzamil@hotmail.com

Essentially, Quick Wins are identified to be addressed first, beginning with the controls that have "Critical" impact on attack mitigation. After this, the controls with "high", "medium" and "low" impact on attack mitigation should be addressed. For other three controls categories, all critical impact controls should be addressed first in the long term implementation plan. The other controls would be implemented as shown in the figure above. By following the above mentioned implementation roadmap, it can be reasonably assumed that the security posture of the organization would increase first rapidly and then consistently by addressing the sub-control and eventually the critical controls. Effective information system security implementation requires identification, assessment, and prioritization of the most appropriate Information Security Controls (van der Haar & von Solms, 2003). In today's environment where financial constraints are severely hampering new initiatives, the above mentioned approach provides a cost-efficient, high impact strategy for enhancing the information security posture of organizations.

3.2. Assessment Project Steps

"*COBIT 5: Assessor Guide*" defines the steps for performing assessments against COBIT 5 framework. Those steps, as mentioned below, can also be applied for performing assessments from Critical Controls perspective.

3.2.1. Initiation

During the initiation phase, the purpose and scope of the assessment is confirmed. Furthermore, the roles and responsibilities of team members, considerations for constraints and initial planning for the assessment are also performed. A sponsor with adequate authority to engage resources and competencies and to make a decision on the identified areas of improvement should also be identified. A pre-assessment questionnaire can be prepared to gain more understanding of the organization. The questionnaire might include items such as the enterprise unit(s) being reviewed, history of information security breaches, current information technology landscape and awareness of related controls or processes. During the initiation phase, assessment scoping should be done in as much detail as possible in order to reduce the overall effort during the assessment and in the implementation phases. During the scoping process, management's input should be heavily sought to ensure that relevant business drivers and associated stakeholder needs have been adequately considered. Management might prioritize and select only the certain controls for assessment due to the fact they fully acknowledge and accept the absence of any supporting activity for a given control. All such assumptions should be formally confirmed with the management/sponsor and reported as such in the final report. It is also important to determine and identify local assessment coordinator to manage the assessment logistics and interface with various enterprise units or personnel. Assessment team members should also be identified and responsibilities should be communicated. It should be ensured that a balanced set of skills necessary to perform the assessment are included with the team members. The team leader should be competent. Normally, the team should consist of at least two assessors.

3.2.2. Planning

During this phase, the plan describing the details of all activities performed during the assessment is documented. Level of effort required to conduct the assessment is also planned at this stage. The required effort is impacted by the scope of the assessment (how many controls are under review), the assurance and confidence required as well as the target capability required for each control.

Since the 20 critical controls are technical in nature with a lot of emphasis on the automation of controls, a key consideration at this stage is selection of tools that will be used to support the assessment. It is recommended that a tool is selected that can cover the scope of large number of controls. During the planning phase, the competencies of the team performing the assessment will also be judged. If it is determined that the team lacks sufficient knowledge or experience, the alternate arrangements (training, replacement of resources etc.) are done.

A proper plan should also be prepared demonstrating where and how the results of the assessment will be stored. The layout of the report and basic information to include in the report are also discussed and agreed upon. As per ISO/IEC 15504, for an assessment to be compliant, "the assessment input shall be defined prior to the data collection phase of an assessment and approved the sponsor of the assessment or the sponsor's delegated authority". Therefore, the plan should ensure that adequate and appropriate data is collected to support the assessment results.

Once all the details in the plan are finalized, it should be reviewed by the lead assessor and formally approved. The approved plan works as the blueprint for all the activities that need be performed during the course of the assessment.

3.2.3. Briefing

This phase involves meeting with the organization's key persons and providing them with the information about the scope, objectives, methodology and expected outcomes. Furthermore, the assessment team should also be briefed about the details on the assessment to ensure that everyone in the team understands their respective roles and responsibilities.

The briefing phase is also used to ensure management support of the assessment and convey the message unequivocally that the assessment is focused on enhancing the information security posture and not on finding flaws with the people doing their job. The real intent of the assessment is to gauge and enhance the technical security controls in order to better serve the objectives of the organization. It should be stressed that the individuals implementing the technical controls are the main source of knowledge and experience about each control and, therefore, their input in identifying the potential weakness and remediating that weakness is crucial.

It is made clear to all participants that the team performing the assessment would respect the confidentiality of information obtained during the assessment process. Care would also be taken that interviews would not be conducted in intimidating or threatening manner. If an external party or consultants are involved in the assessment, necessary and appropriate confidentiality clauses have been included in the contract.

3.2.4. Data Collection

In order to support the evaluation results of the assessment, objective and unbiased evidences should be obtained in the data collection phase. While obtaining the historical data (e.g. logs), the data collection period should be agreed upon the assessment sponsor and process owner. There might have been significant changes in the technical process (e.g. implementation of a new tool, changes in the business process, hardware or software installations, configuration changes etc.) that has to be taken into consideration as they might have an impact on the assessment results. The data collection should be performed in a systematic manner. The approach should also be repeatable so that any subsequent assessments use the similar method. Otherwise, the results of the assessment might be misleading or confusing. All data collected should be sufficient and reliable to arrive at the results of the assessment. The data collected should also meet the purpose and scope of the assessment. A well-established and understood sampling methodology should be used to ensure that data collected represent the total population of the data landscape. Since today's technology infrastructure easily spawns a large number of machines or systems, it is likely that sampling would be required to arrive at the results. SANS recommends two approaches for sampling (course "Audit 507.1: Auditing Networks, perimeters and systems"). The first approach considers the total population and the acceptable margin of error to arrive at the sample size. The second approach uses the "margin of error calculation" to provide on accuracy of the results by examining the number of items already reviewed and their results (pass or fail). This approach is useful even though the total population size might not be known. By using this sampling technique, different geographically dispersed locations with a large number of computer systems could be included in the assessment as it is not necessary to know the total population. Using the statistical knowledge, the great deal of effort can be saved in arriving at the results that would still provide reasonable degree of assurance and confidence.

Once all data have been collected, consideration should be given to systematically recording the data as there might be a large amount of data that might have been collected. The data recording should be done in such a way so that it is easy to reference at a later time. It is likely that management or process owner might challenge some of the findings of the assessment. It is, at this point, the collected data will be referred to in order to substantiate the rating of each control.

The requirements of data collection might vary depending upon the target capability/maturity indicated by the sponsor of the assessment. If for a control, management have already indicated that rating of level 1 would be acceptable, then only interviews might be sufficient as attainment of level 1 only requires general understanding of the control/process. For higher levels (levels 2 to 5), the focus is more narrow and deep. Therefore, data should be collected and analyzed accordingly. It is also important to consider that data or evidence collected in support of the assessment can be in different shapes and forms. The "Direct Evidence" could be the actual document or the actual results. However, it might not be possible to obtain the direct evidence in all circumstances. In such cases, the assessment team might also consider "Best Evidence". The hearsay (sometimes called "Third party evidence") should be avoided during the assessment.

Although the assessment is not a legal review that could end up in the court of law, the assessment team still should carry out the assessment with the knowledge and consideration for the evidence preservation to ensure that due diligence and due professional care has been taken care of in performing the assessment.

3.2.5. Data Validation

The data validation is performed in two stages. Firstly, the assessment team lead should review the data collected and ensure that data is sufficient, relevant and reliable to assign the rating. It should also be ensured that the data collected would serve the purpose of scope and objectives of the assessment. If there are any inconsistencies in data as a whole, they should be addressed at this stage also. Secondly, the data should also be validated with the process owners and the end users (if applicable). Discrepancies between obtained and validated date should be remediated before progressing further. All underlying problems with the data obtained and lack of availability of any data should be informed to the assessment sponsor. It should be reported that any missing data might have a detrimental impact on the rating although the activities might be performed relevant to the controls or processes under review.

3.2.6. Ratings

By using the methodology and process highlighted in section 3.1, a rating would be assigned to the controls on a scale of 0 to 5. It is understood that a great amount of professional judgment might come into play when the ratings are assigned. However, the assessment team should ensure that consistency is preserved in applying the capability or maturity scale. It is also important to consider the repeatability of the method used to assign the ratings as there might be a re-assessment once the intended enhancements have been implemented. The consensus of the assessment team should also be considered. In case, there are any dissenting views, they should be appropriately recorded for future reference.

3.2.7. Reporting

Once the ratings have been reviewed and validated, the assessment report should be prepared and presented to the sponsor or other stakeholders as appropriate. It is vital to highlight that the report is a point in time assessment and does not, in any shape or form, provide an assurance or opinion on the information security risk management or other aspects of the performance. The main purpose of the report is for all stakeholders to understand the level of IT security capabilities and consider implementing improvement recommendations. It should also be mentioned that the report is solely for internal use only and it is not intended to be provided to external parties without explicit management consent.

At a minimum, the report should include administrative details such as, the start and the end dates, purpose, scope, constraints, identities of project sponsor and the distribution list. Furthermore, an executive summary highlighting the key findings should also be included. Although the executive summary can be provided in a presentation format, the assessment report ideally should be a detailed report providing all the necessary and appropriate information. The "Appendices" should be used to provide supporting information (e.g. screenshots) for the ratings of the control.

The content of the report should be thoroughly reviewed for accuracy and completeness. The findings and recommendations should be relevant, specific and concise. . The phrases such as "it seems that" or "it appears that" should be avoided. Similarly, intensifiers such as "very large" or "key" should be avoided. These phrases can be interpreted quite differently by different people reading the report. Furthermore, the purpose of the assessment should be to bring about positive change and not to assign blame for any failures. Therefore, the focus of the report should be the process rather than people executing the set of activities. The risk or implications for not adequately performing the required activities should also be highlighted. In general, the best practices for issuing such assessment reports should be adhered to.

4. Conclusion

Information systems have become indispensable for conducting business activities for almost all organizations regardless of their location, size or type of business. The data generated, maintained and used by the information systems is of tremendous value to the organizations. Any impairment or loss of data security could have devastating impact on the organizations. Along with bringing enormous benefits, technology has also introduced new risks that should be adequately managed. To manage those risks, organizations invest considerable effort and resources without a real sense of direction. However, there is no assurance that all the efforts commensurate with the recent and relevant real life information security threats. The 20 critical controls, maintained by "Council on CyberSecurity", present a focused and prioritized list of areas that organizations can implement in enhancing their information security posture and for mitigating the risks of latest information security threats. When organizations embark upon the journey for implementing the 20 critical controls, the first step is to perform an initial review to determine their current state. Based upon the results of this review, areas of improvement are identified and implemented. Subsequently, more assessments are performed to demonstrate the improvements that have been accomplished. However, there is no standard way of performing and, more importantly, reporting on the results of the assessment. To avoid ambiguous, confusing or conflicting reports on information security, the concepts presented in ISO 15504 and COBIT 5 PAM can be used as a standardized way of assessing and reporting on the maturity/capability of each control. By doing so, the awareness about the controls maturity would be raised and focused decisions could be made for enhancing the areas of most concern to the organization. Furthermore, the degree of subjectivity is reduced to a greater extent in performing the assessment and reporting on the results.

A suggestion is also made to Council on CyberSecurity to consider modifying the terminology from "Controls" to "Process" as each of 20 areas are, in fact, critical processes that should be implemented, monitored, managed and improved upon for information security perspective.

References

Conboy, K. (2010) *Project failure en masse: a study of loose budgetary control in ISD projects*, European Journal of Information Systems, 19(3), 273-287.

Dwivedi, Y. K., Zinner Henriksen, H., Wastell, D. and De', R. (2013) *Grand Successes and Failures in IT: Public and Private Sectors* - IFIP WG 8.6 International Conference, Springer.

Shanahan, M. (2011) *Introducing the New COBIT Assessment Programme: Why and How It Is Replacing the COBIT Maturity Model,* COBIT Focus, 45-9.

Suer, M. (2013) *COBIT 5 Uses Balanced Scorecard to Drive and Demonstrate Performance Improvement,* COBIT Focus, 15-7.

Herath, T., & Rao, H. R. (2009) *Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness,* Decision Support Systems, 47(2), 154-165.

Al-Ahmad, W., & Mohammad, B. (2013) *Addressing Information Security Risks by Adopting Standards,* International Journal Of Information Security Science, 2(2), 28-43.

Van der Haar, H., & von Solms, R. (2003) *A model for deriving information security controls attribute profiles,* Computers & Security, 22(3), 233-244

COBIT Process Assessment Model (PAM): Using COBIT 5 by ISACA.

COBIT Assessor Guide: Using COBIT 5 by ISACA.

ISO/IEC 15504 Information technology — Process assessment standard.

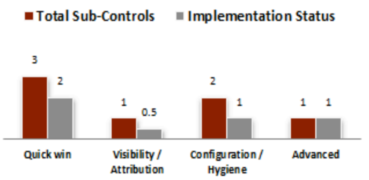
Appendix
Sample Detailed Report by Control

The following show a way by the details about each control could be presented.

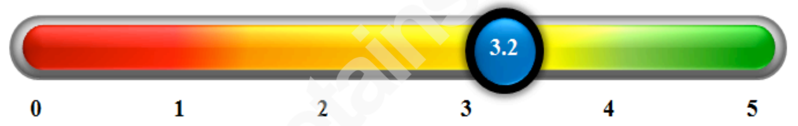
CSC 1 — Inventory of Authorized and Unauthorized Devices

Current Implementation Status

	Total Sub-Controls	Implementation Status
Quick win	3	2
Visibility / Attribution	1	0.5
Configuration / Hygiene	2	1
Advanced	1	1
Total	7	4.5



Overall Implementation Rating



Current State

1. Indicate the details about the current state in a bullet format.
2. Indicate the details about the current state in a bullet format.
3. Indicate the details about the current state in a bullet format.
4. Indicate the details about the current state in a bullet format.
5. Indicate the details about the current state in a bullet format.
6. Indicate the details about the current state in a bullet format.
7. Indicate the details about the current state in a bullet format.
8. Indicate the details about the current state in a bullet format.
9. Indicate the details about the current state in a bullet format.
10. Indicate the details about the current state in a bullet format.

Recommendations for Improvement

Design	Sub Control Ref.	Category
Mention Areas of Improvement for Design	CSC 1-2	Quick win
Mention Areas of Improvement for Design	CSC 1-3	Quick win
Mention Areas of Improvement for Design	CSC 1-4	Visibility/Attribution
Mention Areas of Improvement for Design	CSC 1-6	Configuration/Hygiene

Effectiveness	Automation
1. Mention areas of improvement for effectiveness 2. Mention areas of improvement for effectiveness 3. Mention areas of improvement for effectiveness 4. Mention areas of improvement for effectiveness	1. Mention areas of improvement for automation 2. Mention areas of improvement for automation 3. Mention areas of improvement for automation 4. Mention areas of improvement for automation