ICQ and Audit/Assurance Program for PCI DSS Compliance Program

ICQ and Audit/Assurance Program for PCI DSS Compliance Program

ISACA®
Trust in, and value from, information systems

ISACA®
ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer
ISACA® has designed and created *ICQ and Audit/Assurance Program for PCI DSS Compliance Program* (the "Work") primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide feedback: *www.isaca.org/pci-dss*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

ISBN 978-1-60420-588-6
ICQ and Audit/Assurance Program for PCI DSS Compliance Program

Acknowledgements

ISACA wishes to recognize:

Author
David Lacey, CITP, David Lacey Consulting Ltd., UK

Development Team
Thomas E. Borton, CISA, CISM, CRISC, CISSP, Cost Plus, US
Tien Wei Chng, CISA, CISSP, Visa, Inc., Singapore
Gustavo Garzon, CISM, CRISC, PMP, QSA, PCIP, SEC+, IQ Information Quality, Colombia
Nnamdi Nwosu, CISA, CSTE,CSQA, ITIL, PMP, Moleworth Consulting, Nigeria
Andriy Rybalchenko, CISA, CISM, LLC EastOne, Ukraine
James Seaman, CISM, CRISC, A. Inst. IISP, CCP, QSA, Nettitude Ltd., UK
Eva Sweet, CISA, CISM, ISACA, US

Expert Reviewers
Adesanya Ahmed, CRISC, CGEIT, ACMA, ACPA, Petrovice Resources International, Nigeria
Sujatha Balakrishnan, CISA, NeST Information Technologies Pvt., Ltd. India
Stefan Beissel, Ph.D., CISA, CISSP, EVO Payments International, Germany
Nancy A. Cohen, CPA, CIPP/US, ISACA, USA
Sai K. Honig, CISA, CIA, New Zealand
Ricci Ieong, Ph.D., CISA, CEH, CCSK, CISSP, eWalker Consulting (HK) Ltd., Hong Kong
Shruti Kulkarni, CISA, CRISC, ITIL CCSK, India
Sushila Nair, CISA, CISM, CRISC, CISSP, BT Counterpane, USA
Theodoros Stergiou, CPMM, CCDA, CSSDS, Intracom Telecom, Greece
Siang Jun Julia Yeo, CISA, CRISC, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore

Board of Directors (2015-2016)
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, International President
Rosemary M. Amato, CISA, CMA, CPA, Deloitte, Amsterdam, The Netherlands, Vice President
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, MAICD, Vital Interacts, Australia, Vice President
Robert A. Clyde, CISM, Clyde Consulting LLC, USA, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CPA, CIA, CGAP, CGMA, US House of Representatives, USA, Vice President
Leonard Ong, CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM, CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA, ATD Solution, Singapore, Vice President
Andre Pitkowski, CGEIT, CRISC, OCTAVE, CRMA, ISO27kLA, ISO31kLA, APIT Consultoria de Informatica Ltd., Brazil, Vice President
Eddie Schwartz, CISA, CISM, CISSP-ISSEP, PMP, WhiteOps, USA, Vice President
Gregory T. Grocholski, CISA, SABIC, Saudi Arabia, Past International President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President
Robert E Stroud, CGEIT, CRISC, USA, Past International President
Zubin Chagpar, CISA, CISM, PMP, Amazon Web Services, UK, Director
Matt Loeb, CAE, ISACA, USA, Director
Rajaramiyer Venketaramani Raghu, CISA, CRISC, Versatilist Consulting India, Pvt., Ltd., India, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, FACS CP, BRM Holdich, Australia, Director

ICQ and Audit/Assurance Program for PCI DSS Compliance Program

This document provides the following PCI DSS assurance tools:

1. Internal controls questionnaire (ICQ) that assists enterprises with defining the scope of the assurance engagement and can be used during the exploration period of an audit. **Figure 1** shows the internal controls questionnaire.
2. Audit/assurance program for conducting a PCI DSS Compliance Program assessment, as described in chapter 14 of the *A practical Guide to the Payment Card Industry Data Security Standard (PCI DSS)* book. **Figure 2** shows the audit program that was prepared using the ICQ.

1 PCI DSS Compliance Program ICQ

Figure 1—Internal Controls Questionnaire

Control Objectives/ Questions	Response			Comments	COBIT 5 Reference
	Yes	No	N/A		
1 Development and Maintenance of a Program to Comply With the Standards Framework					
1.1 The organization must include compliance with PCI DSS into the business strategy to set the tone-at-the-top.					
Is PCI DSS compliance reflected in the enterprise strategy?					
Is PCI DSS addressed as a business risk rather than IT risk?					
1.2 The board of directors and executive team must be accountable for the implementation and maintenance of a compliance program to meet PCI DSS requirements.					
Is PCI DSS compliance an element considered while setting and calculating incentives for the board of directors and executive team?					
1.3 The organization must create and maintain a compliance program to meet PCI DSS requirements.					
Is PCI DSS compliance part of the enterprise business goals?					
Is there a formal and documented strategy for achieving and sustaining PCI DSS compliance?					
Has the enterprise defined indicators to measure the compliance program performance?					
1.4 The PCI DSS Compliance Program should include a set of policies that guide employee behavior and performance to ensure that security is part of business as usual.					
Are there defined and documented policies to ensure that employee behavior supports PCI DSS compliance?					
Is human resources involved in developing, distributing and enforcing PCI DSS-related employee policies?					
Does the enterprise document employee acknowledgment of PCI DSS compliance policies?					
1.5 The PCI DSS Compliance Program should include continuous security training awareness plans to ensure that all employees understand the importance of maintaining a secure environment to protect cardholder data.					
Is there a formal process for training employees at time of hiring?					
Is there a formal process for training employees periodically and testing their understanding?					
1.6 The PCI DSS Compliance Program must include plans to hire third-party assessors to evaluate the control environment and help the organization identify gaps and level of compliance.					
Does the enterprise have a formal process for contracting third-party PCI DSS assessors?					
Does the enterprise have a formal process for managing the relationship with third-party PCI DSS assessors?					

Control Objectives/ Questions	Response			Comments	COBIT 5 Reference
	Yes	No	N/A		
Is there documented criteria used to evaluate PCI DSS assessors as part of the contracting process?					
1.7 The PCI DSS Compliance Program must be updated at a minimum every year or every time there is a major change in the organization's operations, the IT infrastructure, the PCI DSS requirements or the external environment.					
Does the enterprise have a formal and documented process for updating the PCI DSS compliance program?					
1.8 The organization must hire and retain employees qualified to implement and maintain the necessary controls to meet PCI DSS compliance.					
Is there documented criteria used to evaluate PCI DSS job candidates as part of the hiring process?					
Does the enterprise provide the necessary training to ensure that employee skills needed to support PCI DSS compliance are current?					
1.9 Service providers must be contractually obligated to comply with security requirements necessary to meet compliance.					
Is compliance with PCI DSS part of the contractual and service level agreement negotiations?					
1.10 Service provider collaboration is recognized as a key success factor and the organization has established policies and procedures to select suppliers and manage the supplier relationship and risk.					
Does the enterprise have a documented process for vendor selection and relationship management?					
Is supplier risk part of the enterprise risk assessment process?					
1.11 Service provider compliance is assessed periodically to ensure that the security perimeter has not been broken.					
Is PCI DSS compliance assessment part of the contractual negotiations?					
Is there a process for assessing third-party PCI DSS compliance?					
2 Implementation of Controls to Meet the Standards Framework					
2.1 The organization must determine the level of compliance required by the PCI SSC.					
Is there a documented process to determine the compliance environment and scope?					
2.2 The organization must assess the current control environment and identify gaps that must be addressed to meet compliance with PCI DSS requirements.					
Is there a documented process to conduct periodic security controls assessments to identify gaps and develop remediation plans?					
2.3 The organization must create a controls framework and implement the necessary controls to meet compliance with PCI DSS.					
Has the enterprise developed a security controls framework that includes controls needed to meet PCI DSS compliance?					
Is the security controls framework reviewed and updated to new requirements?					
2.4 The organization must perform self-assessments at least once a year to ensure that controls are working as intended. Management must prepare remediation plans to close any gaps or weaknesses identified by the self-assessment.					
Is there a formal process to plan and execute PCI DSS compliance self-assessments?					
Are self-assessment results properly documented and shared with stakeholders?					
3 Sustaining Compliance With the Standards Framework					
3.1 The organization must develop and document standards and procedures that help ensure sustainability of the control environment to meet PCI DSS requirements.					
Are policies and procedures developed in a way that compliance can be sustained after it has been achieved?					
3.2 Request to change IT infrastructure components (facilities, network, hardware or software) must be reviewed by management to ensure that changes will not negatively impact the control environment.					
Does the enterprise have a change management					

Control Objectives/ Questions	Response			Comments	COBIT 5 Reference
	Yes	No	N/A		
process that includes the assessment of impact on PCI DSS components as part of the approval and acceptance criteria?					
3.3 Changes in the internal and external environment must be reviewed by management to determine the potential impact to the control environment. Management must prepare remediation plans to address any negative impact resulting from changes.					
Are changes that can impact the PCI DSS environment reviewed and approved by management?					
3.4 New application development must include plans to configure the necessary controls to comply with PCI DSS requirements.					
Does the enterprise have a software development process that includes assessing PCI DSS compliance as part of the development and acceptance requirements?					
Is PCI DSS compliance part of new software testing plans?					
3.5 The organization should engage third parties to perform penetration testing in a proactive way. Management must prepare remediation plans when penetration testing identifies weaknesses.					
Does the enterprise have a formal process for contracting third-party network penetration assessors?					
Does the enterprise have a formal process for managing the relationship with third-party security assessors?					
Is there documented criteria used to evaluate security assessors as part of the contracting process?					
Are network penetration testing results properly documented and shared with stakeholders?					

2 Audit/Assurance Program for PCI DSS Compliance Program

Assurance Engagement: PCI DSS Compliance Program

Assurance Topic

Formal compliance with the Payment Card Industry Data Security Standard (PCI DSS) is carried out either by QSAs or through the completion of an SAQ. The topic of this assessment is the performance and appropriateness of the measures that are implemented to meet the PCI DSS standard, in the context of the enterprise's overall strategy and objectives.

Business Impact and Risk

PCI DSS is a mandatory compliance requirement for all enterprises that process, store, transmit or access cardholder information for any of the major payment card brands. Securing cardholder data is necessary to prevent damaging data breaches, and compliance is essential to avoid penalties from card scheme operators or acquiring banks. Merchants who fail to comply might be forced to pay an extra percentage for noncompliance. There are also fines for storing sensitive authentication data, which is not allowed under the standard. Penalties for data breaches in noncompliant companies can be severe, including large fines and the threat of future exclusion from the payment card network.

Risk resulting from ineffective or incorrect implementation and management of a program to meet and sustain compliance with PCI DSS could result in the following:

- Penalties and fines
- Financial losses due to fraud
- Financial losses resulting from cost associated with security investigations, customer relationship management and emergency fixes
- Revenue loss due to lost consumer confidence
- Reputational damage
- Loss of competitive advantage
- Lawsuits from consumers who experienced identity theft as a result of a security breach

Goal of the Review

The objective of the PCI DSS Compliance Program audit/assurance review is to provide management with an independent assessment relating to the governance, effectiveness and efficiency of PCI DSS security requirements across the enterprise, including the management of services that are delivered by external providers.

Scoping

The scope of this audit/assurance program is to assess the operating effectiveness of an enterprise program to meet and sustain PCI DSS compliance.

Note: This is not a PCI DSS controls assessment. This audit/assurance program has been developed to assess the development and maintenance of a strategy to implement the necessary controls to achieve compliance.

Figure 2—Audit/Assurance Program for PCI DSS Compliance Program

IS Audit and Assurance Program—PCI DSS Compliance Program					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	**Assurance Step**	**Guidance**		**Issue Cross-reference**	**Comments**
A-1	Determine the **stakeholders** of the assurance initiative and their **stake, i.e., the drivers for the assurance engagement.**				
A-1.1	Identify the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.	**Intended user(s) of the assurance report**	**Executive Board and Audit Committee:** Require assurance of the governance, effectiveness and efficiency of PCI DSS security requirements across the enterprise, including the management of services delivered by external providers.		
A-1.2	Identify the interested parties, accountable and responsible for the subject matter over which assurance needs to be provided.	**Accountable and responsible parties for the subject matter**	**Business Executives:** Accountable for guidance on payment card laws and regulations. **IT Steering Committee:** Accountable for guidance on payment card systems and infrastructure, including their design/selection, implementation and management, and the monitoring of service performance, allocation of resources, delivery of benefits/value and management of IT risk. **Business Owners:** Responsible for identifying functional and security requirements, approving the design of payment card systems and managing their operational performance. In partnership with IT management, they are responsible for managing the correct and controlled use of payment card systems, in line with PCI DSS requirements and good industry practices. **IT Management:** Responsible for managing the correct and controlled use of payment card systems, in partnership with business executives and other stakeholders.		
A-2	Determine the assurance **objectives** based on assessment of the internal and external environment/context and of the relevant **risk** and related **opportunities** (i.e., not achieving the enterprise goals).	**Assurance objectives** are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement. **Enterprise objectives** can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically. **Objectives of the assurance engagement** can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals. **Objectives of the assurance engagement** will consider all three value objective components, i.e., delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.				
A-2.1	Understand the **enterprise strategy** and priorities.	Inquire with executive management or through available documentation (corporate strategy, annual report, etc.) about the enterprise strategy and priorities for the coming period, and document them to the extent the process under review is relevant. For example, business initiatives for customer growth, maximization of profits, or IT outsourcing could impact PCI DSS compliance strategy.			

IS Audit and Assurance Program—PCI DSS Compliance Program				
Phase A—Determine Scope of the Assurance Initiative				
Ref.	**Assurance Step**	**Guidance**	**Issue Cross-reference**	**Comments**
A-2.2	Understand the **internal context** of the enterprise.	Identify all internal environmental factors that could influence the **performance and contents of the topic of the audit/assurance program under review.** Examples relevant to PCI DSS might include IT strategy/risks; security roles & responsibilities; system/data ownership; investment appraisal criteria, etc.		
A-2.3	Understand the **external context** of the enterprise.	Identify all external environmental factors that could influence the **performance and contents of the topic of the audit/assurance program under review**. Examples relevant to PCI DSS might include external business & security risks; contractual obligations; supplier compliance status; etc.		
A-2.4	Given the overall assurance objective, translate the identified strategic priorities into concrete objectives for the assurance engagement.	The following goals are retained as **key goals** and **additional goals** to be supported, in reflection of enterprise strategy and priorities:		
		Key goals Enterprise goals: • EG01 Stakeholder value of business investments • EG03 Manage business risk (safeguarding of assets) • EG04 Compliance with external laws and regulations • EG15 Compliance with internal policies IT-related goals: • ITG01 Alignment of IT and business strategy • ITG02 IT compliance and support for business compliance with external laws and regulations • ITG03 Commitment of executive management for IT-related decisions • ITG04 Manage IT-related business risk • ITG05 Realized benefits from IT-enabled investments and service portfolio • ITG07 Delivery of IT services in line with business requirements • ITG10 Security of information, processing infrastructure and applications • ITG11 Optimization of assets, resources and capabilities • ITG13 Delivery of programs delivering benefits, on time, on budget, and meeting requirements and quality standards • ITG15 IT compliance with internal policies • ITG16 Competent and motivated business and IT personnel		
		Additional goals Enterprise goals: • IT-related goals: •		
A-2.5	Define the organizational boundaries of the assurance initiative.	The scope of the cardholder data environment (CDE) will help to determine the business and IT boundaries. All other aspects of scope limitation are identified during phase A-3.		

IS Audit and Assurance Program—PCI DSS Compliance Program				
Phase A—Determine Scope of the Assurance Initiative				
Ref.	**Assurance Step**	**Guidance**	**Issue Cross-reference**	**Comments**
A-3	Determine the **enablers** in scope and the instance(s) of the enablers in scope.	COBIT 5 identifies seven enabler categories. In this section all seven enablers are covered and the assurance professional has the opportunity to select enablers from all categories to obtain the most comprehensive scope for the assurance engagement.		
A-3.1	Define the **Principles, Policies and Frameworks** in scope.	**Principles, policies and frameworks** refer to the communication mechanisms put in place to convey the direction and instructions of the governing bodies and management. In the context of a PCI DSS Compliance review, and taking into account the goals identified in A-2.4, the following principles, policies and frameworks could be considered in scope of the review: • Enterprise governance principles • Decision-making models • Authority levels The following COBIT 5 outputs and inputs are likely to be especially relevant: • ISMS policy (output, APO13). • Connectivity security policy (output, DSS05; input, APO01). • Information architecture model (input, DSS05; output, APO03). • Legal and regulatory compliance requirements (input, MEA03).		
A-3.2	Define which **Processes** are in scope of the review. Processes will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: • Achievement of process goals • Application of process good practices • Existence and quality of work products (inputs and outputs) (insofar not covered by the information items assessments)	*COBIT 5: Enabling Processes* distinguishes a governance domain with a set of processes and a management domain, with four sets of processes. The processes in scope are identified using the goals cascade and subsequent customization. The resulting lists contain key processes and additional processes to be considered during this assurance engagement. Available resources will determine whether they can all be effectively assessed. In the context of this audit/assurance program, processes considered strategic have been listed as key processes. Processes considered operational have been listed as additional processes (for example, BAI06 *Manage Changes* is an operational process that should be part of the Strategic Program to Implement and Sustain PCI DSS compliance).		
		Key processes • EDM01 Ensure Governance Framework Setting and Maintenance • EDM02 Ensure Benefits Delivery • EDM03 Ensure Risk Optimization • EDM04 Ensure Resource Optimization • EDM05 Ensure Stakeholder Transparency • APO01 Manage the IT Management Framework • APO02 Manage Strategy • APO07 Manage Human Resources • APO08 Manage Relationships • APO10 Manage Suppliers • APO12 Manage Risk • APO13 Manage Security • MEA01 Monitor, Evaluate and Assess Performance and Conformance • MEA02 Monitor, Evaluate and Assess System of Internal Controls • MEA03 Monitor, Evaluate and Assess Compliance With External Requirements		
		Additional processes • APO03 Manage Enterprise Architecture • APO04 Manage Innovation • APO05 Manage Portfolio		

IS Audit and Assurance Program—PCI DSS Compliance Program					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	**Assurance Step**	**Guidance**		**Issue Cross-reference**	**Comments**
			• APO06 Manage Budget and Costs • APO09 Manage Service Level Agreements • APO11 Manage Quality • BAI01 Manage Programs and Projects • BAI02 Manage Requirements Definition • BAI03 Manage Solutions Identification and Build • BAI04 Manage Availability and Capacity • BAI05 Mange Organizational Change Enablement • BAI06 Manage Changes • BAI09 Manage Assets • BAI10 Manage Configuration • DSS01 Manage Operations • DSS02 Manage Service Requests and Incidents • DSS03 Manage Problems • DSS04 Manage Continuity • DSS05 Manage Security Services • DSS06 Manage Business Process Controls		
A-3.3	Define which **Organizational Structures** will be in scope. Organizational Structures will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: • Achievement of Organizational Structure goals, i.e., decisions • Application of Organizational Structures good practices	Based on the key processes identified in A-3.2, the following Organizational Structures and functions are considered to be in scope of this assurance engagement, and available resources will determine which ones will be reviewed in detail.			
		Key Organizational Structures	• Board of directors • Chief financial officer (CFO) • Chief information officer (CIO) • Chief information security officer (CISO) • Sales organization • Risk management • Internal audit/compliance • Human resources		
		Additional Organizational Structures	• Software development • IT operations • IT security • Change management • Configuration management • IT services (vendor management) • Legal		
A-3.4	Define the **Culture, Ethics and Behavior** aspects in scope.	In the context of this assignment, the following enterprisewide behaviors are in scope: • Risk- and compliance-aware culture • Accountability • Enterprisewide security awareness • Customer data protection is part of the enterprise strategy • Management proactively monitors risk and action plans progress • Service providers are treated as strategic partners			
A-3.5	Define the **Information items** in scope. Information items will be assessed during	*COBIT 5: Enabling Processes* defines a number of inputs and outputs between processes. Based on the scope of this audit/assurance program the following enabling information items have been identified. Key priorities and availability of resources will determine how many and			

IS Audit and Assurance Program—PCI DSS Compliance Program				
Phase A—Determine Scope of the Assurance Initiative				
Ref.	**Assurance Step**	**Guidance**	**Issue Cross-reference**	**Comments**
	phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: • Achievement of Information goals, i.e., quality criteria of the information items • Application of Information good practices (Information attributes)	which ones will be reviewed in detail. The inputs and outputs for the key processes identified in section A-3.2 can be used as additional information items for this audit/assurance program.		
		Key Information Items • Third-party assessment results • PCI DSS compliance certification • Supplier contracts • IT architecture designs • Network diagrams • Risk analysis results • Penetration testing results • Audit reports • SOC 2 or equivalent reports		
		Additional Information Items • Change management procedures • Configuration management procedures • Vendor management procedures • PCI DSS compliance self-assessment results		
A-3.6	Define the **Services, Infrastructure and Applications** in scope.	In the context of this assignment, and taking into account the goals identified in A-2.4, the following services and related applications and infrastructure could be considered in scope of the review: • Enterprise and IT governance • Change management services and tools • Configuration management services and tools • Data centers • Software development services • Network operations • Hardware management • Security architecture • Development of secured applications • Deploy adequate secured and configured systems • User access and access rights provisioning • Adequate protection against malware, external attacks and intrusion attempts • Monitoring and alert services for security related events		
A-3.7	Define the **People, Skills and Competencies** in scope. Skill sets and competencies will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: • Achievement of skills set goals • Application of skills set and competencies good practices	In the context of this assignment, taking into account key processes and key roles, the following skill sets are included in scope: • Leadership • Enterprise governance • Risk management proficiency • Customer service excellence • Security awareness training • PCI DSS framework, best practices and ancillary documentation proficiency • Information security testing and assessment • Information security experience • Network management experience • Change management experience • Development and implementation of compliance frameworks experience		

IS Audit and Assurance Program—PCI DSS Compliance Program						
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment						
Metrics						
Ref.	**Assurance Steps and Guidance**				**Issue Cross-reference**	**Comments**
B-1	**Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.**					
B-1.1	Obtain (and agree on) metrics for enterprise goals and expected values of the metrics. Assess whether enterprise goals in scope are achieved. *Leverage the list of suggested metrics for the enterprise goals to define, discuss and agree on a set of relevant, customized metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative.* *Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.*					
	The following metrics and expected values are agreed on for the key enterprise goals defined in step A-2.4.					
	Enterprise Goal	**Metric**	**Expected Outcome (Ex)**	**Assessment Step**		
	EG01 Stakeholder value of business investments	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Percent of IT value drivers mapped to business value drivers • Percent of executive management roles with clearly defined accountabilities for IT decisions • Number of times IT is on the board agenda in a proactive manner • Frequency of IT strategy (executive) committee meetings • Rate of execution of executive IT-related decisions	• At least 90 percent of IT strategic goals must be clearly related to enterprise goals. • At least 90 percent of IT value drivers must be mapped to enterprise drivers. • At least 95 percent of executives understand their roles and responsibilities to meet PCI DSS compliance. • At least every six months PCI DSS compliance has been discussed by the board of directors. • Frequent strategic meetings to discuss PCI DSS compliance as part of business as usual. • At least 90 percent of remediation plans have been approved in time to meet objectives set by IT executives.	• Review the enterprise strategy and determine the level of convergence between the business and IT. • Review strategic IT plans and determine how many goals are directly related to meeting enterprise goals. • Select a sample group of executives and assess their level of understanding and commitment to PCI DSS compliance. • Review board of directors past meeting agendas and minutes to assess IT and PCI DSS relevance during those meetings. • Review remediation plans and assess IT executives' scope of authority to review and approve action plans.		
	EG03 Managed business risk (safeguarding of assets)	• Percent of critical business objectives and services covered by risk assessment • Ratio of significant incidents that were not identified in risk assessments vs. total incidents • Frequency of update of risk profile	• At least 85 percent of the cardholder data environment (CDE) is covered by an adequate information security risk assessment. • At least a yearly update to the information security risk profile on the CDE.	• Gather all the information security risk assessments relating to the CDE. • Determine the ratio of assets covered by the information risk assessment vs. the total assets in the CDE. • Obtain the information security risk profile for in the CDE. • Verify the date last updated was less than one year ago.		
	EG04 Compliance with	• Cost of regulatory	• Maximum of one	• Identify all in-scope PCI DSS		

IS Audit and Assurance Program—PCI DSS Compliance Program						
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment						
Metrics						
Ref.	**Assurance Steps and Guidance**				**Issue Cross-reference**	**Comments**
	externals laws and regulations	noncompliance, including settlements and fines • Number of regulatory noncompliance issues causing public comment or negative publicity • Number of regulatory noncompliance issues relating to contractual agreements with business partners	noncompliance issue relating to PCI DSS requirements • Maximum of one noncompliance issue relating to contractual agreements with business partners	requirements. • Verify that all PCI DSS assessments have been satisfactory.		
	EG15 Compliance with internal policies	• Number of incidents related to noncompliance policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices	• Maximum of one incident related to noncompliance with policies related to PCI DSS • 100 percent stakeholders understand and agree with internal policies related to PCI DSS. • 100 percent of policies supported by effective standards and working practices.	• Verify that the organization has not experienced compliance issues during a determined period (e.g., since last review). • Select a sample list of employees and obtain signed policy acknowledgment forms. • Identify all in-scope PCI DSS requirements and match them to standards and procedures.		
B-1.2	Obtain (and agree on) metrics for IT-related goals and expected values of the metrics and assess whether IT-related goals in scope are achieved.					
	The following metrics and expected values are agreed for the key IT-related goals defined in step A-2.4.					
	IT-related Goal	**Metric**	**Expected Outcome**	**Assessment Step**		
	ITG01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programs and services • Percent of IT value drivers mapped to business value drivers	• At least 90 percent of IT strategic goals must be clearly related to enterprise goals. • At least 90 percent of IT value drivers must be mapped to enterprise drivers. • At least 90 percent satisfaction with the level of compliance achieved.	• Review the enterprise strategy and determine the level of convergence between the business and IT. • Review strategic IT plans and determine how many goals are directly related to meeting enterprise goals. • Assess stakeholders' level of satisfaction with PCI DSS compliance status.		
	ITG02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT noncompliance, including settlements and fines, and the impact of reputational loss • Number of IT-related noncompliance issues reported to the board or causing public comment or	• Maximum of one PCI DSS related noncompliance issues reported to the board per year	• Obtain an overview of all PCI DSS-related noncompliance issues in the past year. • Verify impact analysis per issue. • Mark issues reported to the board or causing business impact.		

IS Audit and Assurance Program—PCI DSS Compliance Program						
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment						
Metrics						
Ref.	**Assurance Steps and Guidance**				**Issue Cross-reference**	**Comments**
		embarrassment • Number of noncompliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments				
	ITG03 Commitment of executive management for making IT-related decisions	• Percent of executive management roles with clearly defined accountabilities for IT decisions • Number of times IT is on the board agenda in a proactive manner • Frequency of IT strategy (executive) committee meetings • Rate of execution of executive IT-related decisions	• At least 95 percent of executives understand their roles and responsibilities to meet PCI DSS compliance. • At least every six months PCI DSS compliance has been discussed by the board of directors. • Frequent strategic meetings to discuss PCI DSS compliance as part of business as usual. • At least 90 percent of remediation plans have been approved in time to meet objectives set by IT executives.	• Select a sample group of executives and assess their level of understanding and commitment to PCI DSS compliance. • Review board of directors past meeting agendas and minutes to assess IT and PCI DSS relevance during those meetings. • Review remediation plans and assess IT executives' scope of authority to review and approve action plans.		
	ITG04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programs covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile	• At least 85 percent of business processes in scope for PCI DSS are covered during risk assessments. • At least 95 percent of IT-related risk in scope of PCI DSS must be reviewed during risk assessment exercises. • Based on volume of transactions/incidents, determine the number of incidents that is acceptable. • At least a yearly update to the information security risk profile on the CDE.	• Identify all business processes in scope for PCI DSS and determine if they are covered during risk assessments. • Identify all IT-related risk in scope for PCI DSS and determine if it is covered during risk assessments. • Identify incidents that resulted from risk that was not included in risk assessments. • Review the latest risk profile for cardholder data and determine when it was updated.		
	ITG05 Realized benefits from IT-enabled investments and services portfolio	• Percent of IT-enabled investments where benefit realization is monitored through the full economic life cycle • Percent of IT services	• At least 90 percent of systems are PCI DSS-compliant.	• Review the latest assessment results to determine the level of compliance achieved.		

IS Audit and Assurance Program—PCI DSS Compliance Program						
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment						
Metrics						
Ref.	**Assurance Steps and Guidance**				**Issue Cross-reference**	**Comments**
		where expected benefits are realized • Percent of IT-enabled investments where claimed benefits are met or exceeded				
	ITG07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery	• Based on volume of transactions/incidents, determine the number of incidents that is acceptable. • At least 90 percent of business stakeholders should be satisfied with IT service delivery. • At least 90 percent of users should be satisfied with IT service delivery.	• Determine if the enterprise conducts internal IT service delivery satisfaction surveys and review latest results. • Select a sample list of business stakeholders and users and determine their level of satisfaction.		
	ITG10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines	• Maximum of one security incident per year related to payment card systems causing financial loss or other business impact. • Time to grant, change and remove access privileges is never more than one working day for payment card systems. • A security assessment of PCI DSS compliance is conducted twice a year.	• Obtain an overview of all security incidents in the past year related to payment card systems. • Verify impact analysis per incident. • Mark incidents that caused financial loss or other business impact. • Assess efficiency for the following processes: - Number of security incidents related to payment systems causing financial loss or other business impact - Time to grant, change and remove access privileges, compared to agreed-on service levels for cloud services - Frequency of PCI DSS compliance assessment		
	ITG11 Optimization of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimization assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities	• At least 80 percent of business executives are satisfied with IT performance to implement and sustain a secure environment.	• Select a sample group of business executives and assess their level of satisfaction. • Document any complaints.		
	ITG13 Delivery of programs delivering benefits, on time, on budget, and meeting	• Number of programs/projects on time	• At least 90 percent PCI DSS implementation and	• Review project plans and determine if the completion date and actual costs		

IS Audit and Assurance Program—PCI DSS Compliance Program						
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment						
Metrics						
Ref.	**Assurance Steps and Guidance**				**Issue Cross-reference**	**Comments**
	requirements and quality standards	and within budget • Percent of stakeholders satisfied with program/project quality • Number of programs needing significant rework due to quality defects • Cost of application maintenance vs. overall IT cost	maintenance plans are on time, on budget and meet business defined requirements.	are within the thresholds established by the business.		
	ITG15 IT compliance with internal policies	• Number of incidents related to noncompliance to policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices • Frequency of policies review and update	• Maximum of one incident related to noncompliance with policies related to PCI DSS. • 100 percent stakeholders understand and agree with internal policies related to PCI DSS. • Policies are reviewed and updated at least on a yearly basis.	• Verify that the organization has not experienced compliance issues during a determined period (e.g., since last review) • Select a sample list of employees and obtain signed policy acknowledgment forms. • Identify all policies related to PCI DSS requirements and determine when they were updated.		
	ITG16 Competent and motivated business and IT personnel	• Percent of staff whose IT-related skills are sufficient for the competency required for their role • Percent of staff satisfied with their IT-related roles • Number of learning/training hours per staff member	• 100 percent of employees hired within the last three months have received information security and PCI DSS compliance awareness training. • 100 percent of staff supporting PCI DSS compliance have successfully achieved their training goals.	• Request a list of employees hired within the last three months and validate their participation in information security and PCI DSS compliance awareness training. • Review employee performance reports and determine if training goals are properly established by management. • Contact HR and request training statistics that demonstrate management's commitment to provide training opportunities.		

IS Audit and Assurance Program—PCI DSS Compliance Program				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Principles, Policies and Frameworks				
Ref.	**Assurance Steps and Guidance**		**Issue Cross-reference**	**Comments**
B-2	Obtain an understanding of the **Principles, Policies and Frameworks** in scope and set suitable assessment criteria. Assess Principles, Policies and Frameworks**.**			
Principles, policies and frameworks: Enterprise governance principles				
B-2.1a	Understand the **Principles, Policies and Frameworks context**. *Obtain and understanding of the overall system of internal control and the associated Principles, Policies and Frameworks*			
B-2.2a	Understand the stakeholders of the **Principles, Policies and Frameworks**. *Understand the stakeholders in the policies. The stakeholders for the policies include those setting the policies and those who need to be in compliance with the policies.*			
B-2.3a	Understand the **goals** for the **Principles, Policies and Frameworks**, and the related **metrics** and agree on expected values. Assess whether the **Principles, Policies and Frameworks** goals (outcomes) are achieved, i.e., assess the effectiveness of the **Principles, Policies and Frameworks**.			
	Goal: The organization has defined, disseminated and deployed management policies supporting **enterprise governance principles**.	Perform the assurance steps using the example criteria described below.		
	Goal	**Criteria**	**Assessment Step**	
	Comprehensiveness	The set of policies is comprehensive in its coverage.	Verify that the set of policies is comprehensive in its coverage.	
	Currency	The set of policies is up to date. This at least requires: • A regular validation of all policies whether they are still up to date • An indication of the policies' expiration date or date of last update	Verify that the set of policies is up to date. This at least requires: • A regular validation of all policies whether they are still up to date • An indication of the policies' expiration date or date of last update	
	Flexibility	The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.	Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.	
	Availability	• Policies are available to all stakeholders. • Policies are easy to navigate and have a logical and hierarchical structure.	• Verify that policies are available to all stakeholders. • Verify that policies are easy to navigate and have a logical and hierarchical structure.	
B-2.4a	Understand the life cycle stages of the **Principles, Policies and Frameworks**, and agree on the relevant criteria. Assess to what extent the **Principles, Policies and Frameworks** life cycle is managed. *The life cycle of the IT-related policies is managed by the Process APO01. The review of this life cycle is therefore equivalent to a process review of process APO01* Manage the IT management framework*.*			
B-2.5a	Understand good practices related to the **Principles, Policies and Frameworks** and expected values. Assess the Principles, Policies and Frameworks design, i.e., assess the extent to which expected good practices are applied. *The assurance professional will, by using appropriate auditing techniques assess the following aspects.*			
	Good Practice	**Criteria**	**Assessment Step**	
	Scope and validity	The scope is described and the validity date is indicated.	Verify that the scope of the framework is described and the validity date is indicated.	
	Exception and escalation	• The exception and escalation procedure is explained and commonly known. • The exception and escalation procedure has not become the *de*	• Verify that the exception and escalation procedure is described, explained and commonly known. • Through observation of a representative sample, verify that the exception and escalation	

IS Audit and Assurance Program—PCI DSS Compliance Program					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
Principles, Policies and Frameworks					
Ref.	**Assurance Steps and Guidance**			**Issue Cross-reference**	**Comments**
		facto standard procedure.	procedure has not become *de facto* standard procedure.		
	Compliance	The compliance checking mechanism and noncompliance consequences are clearly described and enforced.	Verify that the compliance checking mechanism and noncompliance consequences are clearly described and enforced.		
B-2.1 to B-2.5	Repeat steps B-2.1 through B-2.5 for all remaining **Principles, Policies and Frameworks** in scope.				
	Repeat the steps described above for the remaining Principles, Policies and Frameworks: • Decision-making models • Authority levels • ISMS policy (output, APO13) • Connectivity security policy (output, DSS05; input, APO01) • Information architecture model (input, DSS05; output, APO03) • Legal and regulatory compliance requirements (input, MEA03)				

IS Audit and Assurance Program—PCI DSS Compliance Program						
B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment						
Processes						
Ref.	**Assurance Steps and Guidance**				**Issue Cross-reference**	**Comments**
B-3	Obtain understanding of the **Processes** in scope and set suitable assessment criteria: for each process in scope (as determined in step A-3.2), additional information is collected and assessment criteria are defined. Assess the Processes.					
PCI DSS Compliance Program[1]: Development and Maintenance of a Program to Comply With the Standards Framework						
B-3.1a	Understand the **Process context.**					
B-3.2a	Understand the **Process purpose.**					
B-3.3a	Understand all process **stakeholders** and their roles. This is equivalent to understanding the real RACI chart of the process. *Leverage the COBIT 5 RACI charts for the processes in scope to identify any additional stakeholders that will need to be involved in the assessment. In this assurance step, the translation is made between the theoretical RACI chart entry and the real enterprise.*					
	The stakeholders of the process are already defined in the RACI chart as a result of step A-3.3. In addition to those stakeholders, this process relies also on the following function(s), which therefore will need to be involved during the assurance engagement: **Development and Maintenance of a Program to Comply With the Standards Framework** stakeholders					
B-3.4a	Understand the Process **goals** and related **metrics[2]** and define expected Process values (criteria), and assess whether the Process goals are achieved, i.e., assess the effectiveness of the process.					
	The Process **Development and Maintenance of a Program to Comply With the Standards Framework** has eleven defined process goals.		The following activities can be performed to assess whether the goals are achieved.			
	Process Goal	**Related Metrics**	**Criteria/Expected Value**	**Assessment Step**		
	The organization must include compliance with PCI DSS into the business strategy to set the tone-at-the-top.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	The board of directors and executive team must be accountable for the implementation and maintenance of a compliance program to meet PCI DSS requirements.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	The organization must create and maintain a compliance program to meet PCI DSS requirements.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		

[1] The scope of this audit/assurance program is to evaluate the effectiveness of an enterprise PCI DSS compliance program; therefore, the assurance steps have been developed in line with PCI DSS terminology. The testing steps have been mapped to COBIT 5 processes to provide a reference where additional metrics and testing techniques can be found.
Assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found on the ISACA web site at *www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx* and can be included in this audit/assurance program depending on the necessity to include them and on resources available.
[2] For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

IS Audit and Assurance Program—PCI DSS Compliance Program						
B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment						
Processes						
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comments
	The PCI DSS Compliance Program should include a set of policies that guide employee behavior and performance to ensure that security is part of business as usual.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	The PCI DSS Compliance Program should include continuous security training awareness plans to ensure that all employees understand the importance of maintaining a secure environment to protect cardholder data.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	The PCI DSS Compliance Program must include plans to hire third-party assessors to evaluate the control environment and help the organization identify gaps and level of compliance.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	The PCI DSS Compliance Program must be updated at a minimum every year or every time there is a major change in the organization's operations, the IT infrastructure, the PCI DSS requirements or the external environment.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	The organization must hire and retain employees qualified to implement and maintain the necessary controls to meet PCI DSS compliance.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	Service providers must be contractually obligated to comply with security requirements necessary to meet compliance.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	Service provider collaboration is recognized as a key success factor and the organization has established policies and procedures to select suppliers and manage the supplier relationship and risk.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	Service provider compliance is assessed periodically to ensure	*Determine the metrics that can be used to assess the achievement*	*Agree on the expected values for the Process goal metrics, i.e., the*	*In this step, the related metrics for each goal will be reviewed*		

IS Audit and Assurance Program—PCI DSS Compliance Program						
B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment						
Processes						
Ref.	**Assurance Steps and Guidance**				**Issue Cross-reference**	**Comments**
	that the security perimeter has not been broken.	*of the Process goals.*	*values against which the assessment will take place.*	*and an assessment will be made whether the defined criteria are achieved.*		
B-3.5a	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement: Define and agree on the reference process, i.e., determine which base practices a process should at least include. (This usually is just a confirmation of the COBIT 5 processes already identified, unless there is reason for using a different reference process.) Agree on the process practices that should be in place (process design). Assess the **process design**, i.e., assess to what extent: • Expected process practices are applied. • Accountability and responsibility are assigned and assumed.					
	COBIT 5 Processes[3] are described in *COBIT 5: Enabling Processes*. Each Process requires a number of management practices to be implemented, as described in the process description in the same guide. These are: • A sound process design • The reference against which the process will be assessed in phase B with the criteria as mentioned, i.e., all management practices are expected to be fully implemented.	Each practice is typically implemented through a number of activities, and a well-designed process will implement all these practices and activities.				
	Reference Process Practices[4]	**Good Practice**	**Assessment Step**		**Issue Cross-reference**	**Comments**
	EDM01	The organization must include compliance with PCI DSS into the business strategy to set the tone-at-the-top.	• Obtain a copy of the enterprise mission and vision statements and determine if protection of cardholder data is a key goal and part of business as usual. • Interview stakeholders and assess their level of satisfaction with management's commitment to comply with PCI DSS requirements. • Determine if the enterprise has experienced security breaches and what actions have taken place to correct the root cause.			
	EDM01	The board of directors and executive team must be accountable for the implementation and maintenance of a compliance program to meet PCI DSS requirements.	• Determine the level of participation the board has while making decisions that impact processes and technologies that are part of the PCI DSS scope.			
	EDM01 EDM03 MEA03	The organization must create and maintain a compliance program to meet PCI DSS requirements.	• Determine if the enterprise has developed and implemented a program to implement and maintain compliance with PCI DSS. • Identify the main stakeholders of the program and assess their satisfaction with the program. • Identify program owners and assess the group using the organizational structures			

[3] For this audit/assurance program, COBIT 5 processes and their related activities are out of scope. Step B-3.5 describes the good practices and assurance steps for the PCI DSS Compliance Program.

[4] This section lists COBIT 5 activities supporting the assurance steps for the PCI DSS Compliance Program audit/assurance program.

IS Audit and Assurance Program—PCI DSS Compliance Program					
B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comments
			enabler dimensions.		
	APO01	The PCI DSS Compliance Program should include a set of policies that guide employee behavior and performance to ensure that security is part of business as usual.	• Obtain copies of all policies that provide guidance for the processes part of the PCI DSS scope. • Determine how employee acknowledgment is obtained and archived • Inquire about the number of exceptions granted and the reason for granting them. • Inquire how often these policies are refreshed and published. • Assess accessibility to policies and policy owners for clarification.		
	APO07 BAI08	The PCI DSS Compliance Program should include continuous security training awareness plans to ensure that all employees understand the importance of maintaining a secure environment to protect cardholder data.	• Determine training frequency and find out the date of the last training. • Determine how employee acknowledgment is obtained and archived • Select a sample list of employees and assess their understanding and satisfaction with the training provided. • Determine if the enterprise has developed and published a security manual that helps employees perform their duties in accordance with PCI DSS requirements. • Determine the number of security incidents caused by employee errors that could have been prevented with training.		
	APO12 APO13 MEA03	The PCI DSS Compliance Program must include plans to hire third-party assessors to evaluate the control environment and help the organization identify gaps and level of compliance.	• Request the latest PCI DSS evaluation report. • Request remediation plans for any deficiencies documented in the report. • Inquiry what the frequency is of third-party assessments.		
	EDM01	The PCI DSS Compliance Program must be update at a minimum every year or every time there is a major change in the organization's operations, the IT infrastructure, the PCI DSS requirements or the external environment.	• Determine if the enterprise has developed and documented a formal process for the maintenance of the PCI DSS Compliance program. • Obtain a copy of the latest documentation and review the date when it was updated. • Compare the PCI DSS Compliance program to the current PCI DSS requirements and determine if there are gaps.		
	APO07	The organization must hire and retain employees qualified to implement and maintain the necessary controls to meet PCI DSS compliance.	• Refer to section B-8 to obtain the testing techniques for COBIT 5 process APO07 *Manage Human Resources*		
	APO10	Service providers must be contractually obligated to comply with security requirements necessary to meet compliance.	• Obtain all service performance reports and evaluations. • Interview service managers. • Verify the expected values. • For any supplier failing to meet the agreed requirements, verify whether this is a recurring trend. • Determine the root cause of any trend, and suggest actions for improvement, or consider another supplier.		
	APO10	Service provider collaboration is recognized as a key success factor and the organization has established policies and	• Obtain the meeting minutes from all the supplier meetings. • Verify that the meetings were held on a regular basis. • Verify that action points from the previous meeting have been addressed, previous period supplier performance was discussed and new action/improvement points are set		

IS Audit and Assurance Program—PCI DSS Compliance Program					
B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
Processes					
Ref.	**Assurance Steps and Guidance**			**Issue Cross-reference**	**Comments**
		procedures to select suppliers and manage the supplier relationship and risk.	forward.		
	APO10	Service provider compliance is assessed periodically to ensure that the security perimeter has not been broken.	• Verify that 100 percent of the noncompliant requirements were risk assessed and resolved.		
B-3.6a	Agree on the **process work products**[5] (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.				
	The Process **Compliance With the Standards Framework** identifies a set of inputs and outputs for the different management practices. The most relevant of these work products (and those not assessed as Information items in scope in section A-3.5) are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.		Criteria: All listed work products should demonstrably exist and be used.		
	Process Practice	**Work Product**	**Assessment Step**		
	Compliance with the Standards Framework	• Mission/vision statement • PCI DSS compliance policies • Service provider contracts • PCI DSS compliance assessment reports • Remediation plans • Infrastructure designs • Information security policy • Hiring policies and procedures • Job descriptions • Employee handbook	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.			
B-3.7a	Agree on the **process capability level** to be achieved by the process.				
	This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.				
PCI DSS Compliance Program: Implementation of Controls to Meet the Standards Framework					
B-3.1b	Understand the **Process context.**				
B-3.2b	Understand the **Process purpose.**				
B-3.3b	Understand all process **stakeholders** and their roles.				
	Implementation of Controls to Meet the Standards Framework stakeholders				
B-3.4b	Understand the **Process goals** and related **metrics**[6] and define expected Process values (criteria), and assess whether the Process goals are achieved, i.e., assess the effectiveness of the process.				
	The Process **Implementation of Controls to Meet the Standards Framework** has four defined process goals.		The following activities can be performed to assess whether the goals are achieved.		
	Process Goal	**Related Metrics**	**Criteria/Expected Value**	**Assessment Step**	

[5] For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*.
[6] For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

IS Audit and Assurance Program—PCI DSS Compliance Program						
B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment						
Processes						
Ref.	**Assurance Steps and Guidance**				**Issue Cross-reference**	**Comments**
	The organization must determine the level of compliance required by the PCI SSC.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	The organization must assess the current control environment and identify gaps that must be addressed to meet compliance with PCI DSS requirements.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	The organization must create a controls framework and implement the necessary controls to meet compliance with PCI DSS.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	The organization must perform self-assessments at least once a year to ensure that controls are working as intended. Management must prepare remediation plans to close any gaps or weaknesses identified by the self-assessment.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
B-3.5b	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:					
	Reference Process Practices[7]	**Good Practice**	**Assessment Step**			
	EDM01 APO01 APO12 MEA03	The organization must determine the level of compliance required by the PCI council.	• Determine if the level of compliance has been defined using PCI guidelines for different merchant categories. • Request documentation that describes the compliance scope (processes, locations, networks, systems, etc.).			
	APO12 APO13	The organization must assess the current control environment and identify gaps that must be addressed to meet compliance with PCI DSS requirements.	• Request risk assessment results for processes and technologies that are in the PCI DSS scope. • Request remediation plans for gaps identified during risk and control environment assessments. • Validate that remediation plans have been implemented and tested to ensure controls work as intended.			
	APO13	The organization must create a controls framework and implement the necessary controls to meet compliance with PCI DSS.	• Request documentation that describes the controls framework developed to implement a secure environment that meets PCI DSS requirements. • Identify any gaps between the framework and the latest PCI DSS requirements.			

[7] This section lists COBIT 5 activities supporting the assurance steps for the PCI DSS Compliance Program audit/assurance program.

IS Audit and Assurance Program—PCI DSS Compliance Program						
B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment						
Processes						
Ref.	**Assurance Steps and Guidance**				**Issue Cross-reference**	**Comments**
	APO12 MEA01	The organization must perform self-assessments at least once a year to ensure that controls are working as intended. Management must prepare remediation plans to close any gaps or weaknesses identified by the self-assessment.	• Request the results from the latest self-assessment. • Request remediation plans for gaps identified during the self-assessment. • Validate that remediation plans have been implemented and tested to ensure controls work as intended. • Determine if self-assessments include all connections to service providers. • Request the latest SOC 2 reports provided by third parties that store, process or transmit cardholder data.			
B-3.6b	Agree on the **process work products**[8] (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.					
	The Process **Implementation of Controls to Meet the Standards Framework** identifies a set of inputs and outputs for the management practices. The most relevant of these work products (and those not assessed as Information items in scope in section A-3.5) are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.			Criteria: All listed work products should demonstrably exist and be used.		
	Process Practice	**Work Products**		**Assessment Step**		
	Implementation of Controls to Meet the Standards Framework	• PCI DSS scope documentation • Controls framework • Self-assessment reports • Remediation plans • Service provider reports • Network diagrams		Apply appropriate audit techniques to determine the existence and appropriate use of each work product.		
B-3.7b	Agree on the **process capability level** to be achieved by the process.					
	This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.					
PCI DSS Compliance Program: Sustaining Compliance With the Standards Framework						
B-3.1c	Understand the **Process context.**					
B-3.2c	Understand the **Process purpose.**					
B-3.3c	Understand all process **stakeholders** and their roles.					
	Sustaining Compliance With the Standards Framework stakeholders:					
B-3.4c	Understand the **Process goals** and related **metrics**[9] and define expected Process values (criteria), and assess whether the Process goals are achieved, i.e., assess the effectiveness of the process.					
	The Process **Sustaining Compliance With the Standards Framework** has five defined process goals.		The following activities can be performed to assess whether the goals are achieved.			
	Process Goal	**Related Metrics**	**Criteria/Expected Value**	**Assessment Step**		
	The organization must develop and document standards and procedures that help ensure	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the*	*In this step, the related metrics for each goal will be reviewed and an assessment will be*		

[8] For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*.
[9] For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

IS Audit and Assurance Program—PCI DSS Compliance Program						
B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment						
Processes						
Ref.	**Assurance Steps and Guidance**				**Issue Cross-reference**	**Comments**
	sustainability of the control environment to meet PCI DSS requirements.		*assessment will take place.*	*made whether the defined criteria are achieved.*		
	Request to change IT infrastructure components (facilities, network, hardware or software) must be reviewed by management to ensure that changes will not negatively impact the control environment.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	Changes in the internal and external environment must be reviewed by management to determine the potential impact to the control environment. Management must prepare remediation plans to address any negative impact resulting from changes.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	New application development must include plans to configure the necessary controls to comply with PCI DSS requirements.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
	The organization should engage third parties to perform penetration testing in a proactive way. Management must prepare remediation plans when penetration testing identifies weaknesses.	*Determine the metrics that can be used to assess the achievement of the Process goals.*	*Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.*	*In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.*		
B-3.5c	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:					

Reference Process Practices[10]	**Good Practice**	**Assessment Step**		
DSS01	The organization must develop and document standards and procedures that help ensure sustainability of the control environment to meet PCI DSS requirements.	• Review standards and procedures that have been developed to ensure that IT operations align with PCI DSS requirements. • Request exceptions that have been granted and inquire the reason for the exception.		
BAI06	Request to change IT infrastructure components	• Review change management policies and procedures to determine if the appropriate level of approval and testing is performed to ensure that controls to meet PCI DSS		

[10] This section lists COBIT 5 activities supporting the assurance steps for the PCI DSS Compliance Program audit/assurance program.

IS Audit and Assurance Program—PCI DSS Compliance Program					
B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
Processes					
Ref.	**Assurance Steps and Guidance**			**Issue Cross-reference**	**Comments**
		(facilities, network, hardware or software) must be reviewed by management to ensure that changes will not negatively impact the control environment.	requirements are not weakened or disabled. • Request a sample of change request forms and assess compliance with change management policies and procedures. Request testing results when possible.		
		Changes in the internal and external environment must be reviewed by management to determine the potential impact to the control environment. Management must prepare remediation plans to address any negative impact resulting from changes.	• Review organizational change policies and procedures to determine if appropriate level of approval and assessment is performed to ensure that the controls environment is not weakened. • Inquire about the latest organizational change and determine if potential impact on PCI DSS compliance was properly assessed and addressed.		
	BAI02 BAI03	New application development must include plans to procure/configure the necessary controls to comply with PCI DSS requirements.	• Review software development policies and procedures to determine if security controls are part of the business requirements. • Request test results that demonstrate that security controls are part of any testing prior to software being promoted to the production environment. • Review third-party contracts and service level agreements (SLAs) to determine if security controls are included in the enterprise requirements for software development and maintenance.		
	APO12 APO13	The organization should engage third parties to perform penetration testing in a proactive way. Management must prepare remediation plans when penetration testing identifies weaknesses.	• Review policies and procedures for conducting penetration testing. • Request the results of the latest test. • Review remediation plans to address any weaknesses identified during the penetration testing. • Inquire if a test is conducted after weaknesses are addressed to evaluate improvement. • Inquire about the frequency of penetration testing. • Determine if the enterprise has a rotation plan to use different service providers to conduct penetration testing or if the same entity is contracted.		
B-3.6c	Agree on the **process work products**[11] (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.				
	The Process **Sustaining Compliance With the Standards Framework** identifies a set of inputs and outputs for the different management practices. The most relevant of these work products (and those not assessed as Information items in scope in section A-3.5) are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.		Criteria: All listed work products should demonstrably exist and be used.		
	Process Practice	**Work Products**	**Assessment Step**		
	Sustaining Compliance With the Standards Framework	• Change management policies and procedures • Change request forms • Process exception forms • Organizational change risk assessments • Software development policies and procedures • Service provider contracts and SLAs	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.		

[11] For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*.

IS Audit and Assurance Program—PCI DSS Compliance Program					
B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
Processes					
Ref.	**Assurance Steps and Guidance**			**Issue Cross-reference**	**Comments**
		• Penetration testing results • Remediation plans			
B-3.7c	Agree on the **process capability level** to be achieved by the process.				
	This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.				

IS Audit and Assurance Program—PCI DSS Compliance Program			
Phase B —Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Organizational Structures			
Ref.	**Assurance Steps and Guidance**	**Issue Cross-reference**	**Comments**
B-4	Obtain understanding of each **Organizational Structure** in scope and set suitable assessment criteria: For each **Organizational Structure** in scope (as determined in step A-3.3), additional information is collected and assessment criteria are defined. Assess the **Organizational Structure.**		
Organizational Structure: Board of Directors			
B-4.1a	Understand the **Organizational Structure** context. *Identify and document all elements that can help to understand the context in which the* **board of directors** *organization has to operate, including:* • *The overall organization* • *Management/process framework* • *History of the role/structure* • *Contribution of the Organizational Structure to achievement of goals*		
B-4.2a	Understand all **stakeholders** of the **Organizational Structure**/function. *Determine through documentation review (policies, management communications, etc.) the key stakeholders of the* **board of directors** *organization.* • *Incumbent of the role and/or members of the Organizational Structure* • *Other key stakeholders affected by the decisions of the Organizational Structure/role*		
B-4.3a	Understand the **goals** of the **Organizational Structure**, the related **metrics** and agree on expected values. Understand how these goals contribute to the achievement of the enterprise goals and IT-related goals.		
	Organizational Structure Goal / **Assessment Step**		
	Determine through interviews with key stakeholders and documentation review the goals of the **board of directors**, i.e., **the decisions for which they are accountable.**[12,13] This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: • Identify the decisions made by the Organizational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by assessing whether: - They have contributed to the achievement of the IT-related and enterprise goals as anticipated. - Decisions are duly executed on a timely basis.		
B-4.4a	Agree on the expected good practices for the **Organizational Structure** against which it will be assessed. Assess the **Organizational Structure design**, i.e., assess the extent to which expected **good practices** are applied.		
	Good Practice / **Criteria** / **Assessment Step**		
	Operating principles • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful.		
	Composition The board of directors' composition is balanced and complete, i.e., all required Assess whether the board of directors' composition is balanced and complete, i.e.,		

[12] The RACI charts in *COBIT 5: Enabling Processes* can be leveraged as a starting point for the expected goals of a role or Organizational Structure.

[13] The Organizational Structure/role as described may not exist under the same name in the enterprise; in that case, the closest Organizational Structure assuming the same responsibilities and accountability should be considered.

IS Audit and Assurance Program—PCI DSS Compliance Program					
Phase B —Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
Organizational Structures					
Ref.	**Assurance Steps and Guidance**			**Issue Cross-reference**	**Comments**
		stakeholders are sufficiently represented.	all required stakeholders are sufficiently represented.		
	Span of control	• The span of control of the board of directors is defined. • The span of control is adequate, i.e., the board of directors has the right to make all decisions it should. • The span of control is in line with the overall enterprise governance arrangements.	• Verify whether the span of control of the board of directors is defined. • Assess whether the span of control is adequate, i.e., the board of directors has the right to make all decisions it should. • Verify and assess whether the span of control is in line with the overall enterprise governance arrangements.		
	Level of authority/decision rights	• Decision rights of the board of directors are defined and documented. • Decision rights of the board of directors are respected and complied with (also a culture/behavior issue).	• Verify that decision rights of the board of directors are defined and documented. • Verify whether decision rights of the board of directors are complied with and respected.		
	Delegation of authority	Delegation of authority is implemented in a meaningful way.	Verify whether delegation of authority is implemented in a meaningful way.		
	Escalation procedures	Escalation procedures are defined and applied.	Verify the existence and application of escalation procedures.		
B-4.5a	Understand the life cycle and agree on expected values. Assess the extent to which the **Organizational Structure life cycle** is managed.				
	Life Cycle Element	**Criteria**	**Assessment Step**		
	Mandate	• The board of directors is formally established. • The board of directors has a clear, documented and well-understood mandate.	• Verify through interviews and observations that the board of directors is formally established. • Verify through interviews and observations that the board of directors has a clear, documented and well-understood mandate.		
	Monitoring	• The performance of the board of directors and its members should be regularly monitored and evaluated by competent and independent assessors. • The regular evaluations should result in the required continuous improvements to the board of directors, either in its composition, mandate or any other parameter.	• Verify whether the performance of the board of directors and its members is regularly monitored and evaluated by competent and independent assessors. • Verify whether the regular evaluations have resulted in improvements to the board of directors, in its composition, mandate or any other parameter.		
B-4.1 to B-4.5	Repeat steps B-4.1 through B-4.5 for all remaining **Organizational Structures** in scope.				
	Repeat the steps described above for the remaining Organizational Structures: • Chief financial officer (CFO) • Chief information officer (CIO) • Chief information security officer (CISO)				

IS Audit and Assurance Program—PCI DSS Compliance Program			
Phase B —Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Organizational Structures			
Ref.	**Assurance Steps and Guidance**	**Issue Cross-reference**	**Comments**
	• Sales organization • Risk management • Internal audit/compliance • Human resources		

IS Audit and Assurance Program—PCI DSS Compliance Program				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Culture, Ethics and Behavior				
Ref.	**Assurance Step and Guidance**		**Issue Cross-reference**	**Comments**
B-5	Obtain understanding of the **Culture, Ethics and Behavior** in scope. Assess Culture, Ethics and Behavior.			
Culture, Ethics and Behavior: Risk- and compliance-aware culture				
B-5.1a	Understand the **Culture, Ethics and Behavior context**. • *What the overall corporate Culture is like* • *Understand the interconnection with other enablers in scope:* - *Identify roles and structures that could be affected by the Culture.* - *Identify processes that could be affected by Culture, Ethics and Behavior, including any processes in scope of the review.*			
B-5.2a	Understand the major **stakeholders** of the **Culture, Ethics and Behavior**: **Risk and compliance aware culture** *Understand to whom the behavior requirements will apply, i.e., understand who embodies the roles/structures expected to demonstrate the correct set of Behaviors. This is usually linked to the roles and Organizational Structures identified in scope.*			
B-5.3a	Understand the **goals** for the **Culture, Ethics and Behavior**, and the related **metrics** and agree on expected values. Assess whether the **Culture, Ethics and Behavior goals** (outcomes) are achieved, i.e., assess the effectiveness of the Culture, Ethics and Behavior.			
	In the context of **risk- and compliance-aware culture**, the following **Culture, Ethics and Behavior** are desired:	Culture and especially Behaviors are associated to individuals and the Organizational Structures of which they are a part; therefore, by using appropriate auditing techniques, the assurance professional will: • Identify individuals who must comply with the Behaviors under review. • Identify the Organizational Structures involved. • Assess whether desired Behaviors can be observed. • Assess whether undesirable Behaviors are absent. For a representative sample of individuals, perform the following assessment steps.		
	Desired Behavior (Culture, Ethics and Behavior Goal)	**Assessment Step**		
	The enterprise is aware of the compliance requirements it must abide.			
	Employees understand their role in maintaining compliance.			
	Identified risk is properly addressed.			
	Controls are in place to ensure compliance with internal and external requirements.			
B-5.4a	Understand the life cycle stages of the **Culture, Ethics and Behavior**, and agree on the relevant criteria. Assess to what extent the Culture, Ethics and Behavior life cycle is managed.			
	(This aspect is already covered by the assessment of the good practices, hence no additional separate assurance steps are defined here.)			
B-5.5a	Understand good practice when dealing with **Culture, Ethics and Behavior**, and agree on relevant criteria. Assess the Culture, Ethics and Behavior design, i.e., assess to what extent expected good practices are applied.			
	Good Practice	**Criteria**	**Assessment Step**	
	Communication, enforcement and rules	Existence and quality of the communication	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.	
	Incentives and rewards	Existence and application of appropriate rewards and incentives	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.	

IS Audit and Assurance Program—PCI DSS Compliance Program					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
Culture, Ethics and Behavior					
Ref.	**Assurance Step and Guidance**			**Issue Cross-reference**	**Comments**
	Awareness	Awareness of desired Behaviors	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.		
B-5.1 to B-5.5	Repeat steps B-5.1 through B-5.5 for all remaining **Culture, Ethics and Behavior** in scope.				
	Repeat the steps described above for the remaining Culture, Ethics and Behavior: • Accountability • Enterprisewide security awareness • Customer data protection is part of the enterprise strategy • Management proactively monitors risk and action plans progress • Service providers are treated as strategic partners				

IS Audit and Assurance Program—PCI DSS Compliance Program			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Information Items			
Ref.	**Assurance Steps and Guidance**	**Issue Cross-reference**	**Comments**
B-6	Obtain understanding of the Information Items in scope. Assess Information Items.		
Information Item: Third-party assessment results			
B-6.1a	Understand the Information item **context**: • *Where and when is it used?* • *For what purpose is it used?* • *Understand the connection with other enablers in scope, e.g.:* - *Used by which processes?* - *Which Organizational Structures are involved?* - *Which services/applications are involved?*		
B-6.2a	Understand the major **stakeholders** of the **Information item**. *Understand the stakeholders for the Information item, i.e., identify the:* • *Information producer* • *Information custodian* • *Information consumer* *Stakeholders should be at the appropriate organizational level.*		
B-6.3a	Understand the major quality criteria for the Information item, the related metrics and agree on expected values. Assess whether the **Information item quality criteria** (outcomes) are achieved, i.e., assess the effectiveness of the Information item.		

Leverage the COBIT 5 Information enabler model[14] focusing on the quality goals description to select the most relevant Information quality criteria for the Information item at hand. Document expectations regarding information criteria. The COBIT 5 Information enabler model identifies 15 different quality criteria—although all of them are relevant, it is nonetheless possible and recommended to focus on a subset of the most important criteria for the Information item at hand.

Mark the quality dimensions with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.

The assurance professional will, by using appropriate auditing techniques, verify all quality criteria in scope and assess whether the criteria are met.

Quality Dimension	Key Criteria	Description	Assessment Step		
Accuracy	✓				
Objectivity					
Believability					
Reputation	✓				
Relevancy	✓				
Completeness	✓				
Currency	✓				
Amount of information	✓				
Concise representation	✓				
Consistent representation					
Interpretability					
Understandability	✓				
Manipulation					
Availability	✓				

[14] COBIT 5 framework, appendix G, p.81-84

IS Audit and Assurance Program—PCI DSS Compliance Program						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment						
Information Items						
Ref.	**Assurance Steps and Guidance**				**Issue Cross-reference**	**Comments**
	Restricted access					
B-6.4a	Understand the **life cycle** stages of the Information item, and agree on the relevant criteria. Assess to what extent the **Information item life cycle** is managed.					
	The life cycle of any Information item is managed through several business and IT-related processes. The scope of this review already includes a review of (IT-related) processes so this aspect does not need to be duplicated here. • When the Information item is internal to IT, the process review will have covered the life cycle aspects sufficiently. • When the Information item also involves other stakeholders outside IT or other non-IT processes, some of the life cycle aspects need to be assessed. Mark the life cycle stages with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.					
	Life Cycle Stage	**Key Criteria**	**Description**	**Assessment Step**		
	Plan	✓				
	Design	✓				
	Build/acquire	✓				
	Use/operate	✓				
	Evaluate/monitor	✓				
	Update/dispose	✓				
B-6.5a	Understand important attributes of the Information item and expected values. Assess the **Information item design**, i.e., assess the extent to which expected **good practices** are applied.					
	Good practices for Information items are defined as a series of attributes for the **Information item.**[15] The assurance professional will, by using appropriate audit techniques, verify all attributes in scope and assess whether the attributes are adequately defined. Mark the attributes with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.					
	Attribute	**Key Criteria**	**Description**	**Assessment Step**		
	Physical					
	Empirical					
	Syntactic					
	Semantic					
	Pragmatic	✓				
	Social					
B-6.1 to B-6.5	Repeat steps B-6.1 through B-6.5 for all remaining **Information items** in scope.					
	Repeat the steps described above for the remaining Information items: • PCI DSS compliance certification • Supplier contracts • IT architecture designs • Network diagrams • Risk analysis results • Penetration testing results • Audit reports • SOC 2 or equivalent reports • Change management procedures					

[15] COBIT 5 framework, appendix G, p. 81-84

IS Audit and Assurance Program—PCI DSS Compliance Program			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Information Items			
Ref.	**Assurance Steps and Guidance**	**Issue Cross-reference**	**Comments**
	• Configuration management procedures • Vendor management procedures • PCI DSS compliance self-assessment results		

IS Audit and Assurance Program—PCI DSS Compliance Program					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
Services, Infrastructure and Applications					
Ref.	**Assurance Steps and Guidance**			**Issue Cross-reference**	**Comments**
B-7	Obtain understanding of the **Services, Infrastructure and Applications** in scope. Assess Services, Infrastructure and Applications.				
Services, Infrastructure and Applications: Enterprise and IT Governance					
B-7.1a	Understand the **Services, Infrastructure and Applications** context. *Understand the organizational and technological context of this service. Refer to step A-2.2 and A-2.3 and re-use that information to understand the significance of this Service, Infrastructure and Application.*				
B-7.2a	Understand the major **stakeholders** of the **Services, Infrastructure and Applications**. *Understand who will be the major stakeholders of the service, i.e., the sponsor, provider and users. Stakeholders will include a number of organizational roles but could also link to Processes.*				
B-7.3a	Understand the major **goals** for the **Services, Infrastructure and Applications**, the related **metrics** and agree on expected values. Assess whether the Services, Infrastructure and Applications goals (outcomes) are achieved, i.e., assess the effectiveness of the Services, Infrastructure and Applications.				
	Goal	**Criteria**	**Assessment Step**		
	Service description	• The Service is clearly described. • Roles and responsibilities are clearly defined. • The Service is available to all potential stakeholders.	• Verify that the Service exists and is clearly described. • Verify that roles and responsibilities are clearly defined. • Assess the quality of the Service description and of the Service offered. • Verify the accessibility of the Service to all potential stakeholders.		
	Service level definition	Service levels are defined for : • Quality of the service deliverables • Ease to request the service • Timeliness	• Verify that the following aspects are dealt with in the Service level definitions: - Quality of the Service deliverables - Ease to request the service - Timeliness • Verify to what extent Service levels are achieved.		
	Contribution to related enablers, IT-related and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.		
B-7.4a	Understand good practice related to the Services, Infrastructure and Applications and expected values. Assess the **Services, Infrastructure and Applications** design, i.e., assess to what extent expected good practices are applied. *Leverage the description of Services, Infrastructure and Applications in the COBIT 5 framework[16] to identify good practices related to Services, Infrastructure And Applications. In general the following practices need to be implemented:* • *Buy/build decision needs to be taken.* • *Use of the Service needs to be clear.*				
	Good Practice	**Criteria**	**Assessment Step**		
	Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the	• Verify that a formal decision—based on a business case—was taken regarding		

[16] COBIT 5 framework, appendix G, p.85-86

IS Audit and Assurance Program—PCI DSS Compliance Program					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
Services, Infrastructure and Applications					
Ref.	**Assurance Steps and Guidance**			**Issue Cross-reference**	**Comments**
		sourcing of the Service.	the sourcing of the Service. • Verify the validity and quality of the business case. • Verify that the sourcing decision has been duly executed.		
	Use	The use of the Service needs to be clear: • When it needs to be used and by whom • The required compliance levels with the Service's output	• Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be used. • Verify that actual use is in line with requirement above. • Verify that the actual Service output is adequately used. • Verify that Service levels are monitored and achieved.		
B-7.1 to B-7.4	Repeat steps B-7.1 through B-7.4 for all remaining **Services, Infrastructure and Applications** in scope.				
	Repeat the steps described above for the remaining Services, Infrastructure and Applications: • Change management services and tools • Configuration management services and tools • Data centers • Software development services • Network operations • Hardware management • Security architecture • Development of secured applications • Deploy adequate secured and configured systems • User access and access rights provisioning • Adequate protection against malware, external attacks and intrusion attempts • Monitoring and alert services for security related events				

IS Audit and Assurance Program—PCI DSS Compliance Program				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
People, Skills and Competencies				
Ref.	**Assurance Steps and Guidance**		**Issue Cross-reference**	**Comments**
B-8	Obtain understanding of the **People, Skills and Competencies** in scope. Assess People, Skills and Competencies.			
People, Skill and Competency: Leadership				
B-8.1a	Understand the **People, Skills and Competencies** context. *Understand the context of the Skill/Competency, i.e.,:* • *Where and when is it used?* • *For what purpose is it used?* • *Understand the connection with other enablers in scope, e.g.:* - *In which roles and structures is the Skill/Competency used? (See also B-4.1.)* *Which behaviors are associated with the Skill/Competency?*			
B-8.2a	Understand the major **stakeholders** for the People, Skills and Competencies. *Identify to whom in the organization the skill requirement applies.*			
B-8.3a	Understand the major **goals** for the **People, Skills and Competencies**, the related **metrics** and agree on expected values. Assess whether the **People, Skills and Competencies goals** (outcomes) are achieved, i.e., assess the effectiveness of the People, Skills and Competencies. For the People, Skills and Competencies: **Leadership**, the following goals and associated criteria can be addressed.			
	Goal	**Criteria**	**Assessment Step**	
	Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.	
	Education			
	Qualification			
	Knowledge			
	Technical skills			
	Behavioral skills			
	Number of people with appropriate skill level			
B-8.4a	Understand the **life cycle** stages of the **People, Skills and Competencies**, and agree the relevant criteria. Assess to what extent the People, Skills and Competencies life cycle is managed.			
	For the People, Skills and Competencies at hand, the life cycle phases and associated criteria can be expressed in function of the process APO07.		For the People, Skills and Competencies at hand the assurance professional will perform the following assessment steps.	
	Life Cycle Element	**Criteria**	**Assessment Step**	
	Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.	
	Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill.	
		Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.	

IS Audit and Assurance Program—PCI DSS Compliance Program					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
People, Skills and Competencies					
Ref.	**Assurance Steps and Guidance**			**Issue Cross-reference**	**Comments**
	Build	Practice APO07.03 activity 4 (Identify gaps between required and available skills and develop action plans to address them on an individual and collective basis, such as training [technical and behavioral skills], recruitment, redeployment and changed sourcing strategies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 4 is implemented in relation to this skill.		
	Operate	Practice APO07.03 activity 5 (Develop and deliver training programs based on organizational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct and security.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 5 is implemented in relation to this skill.		
	Evaluate	Practice APO07.03 activity 6 (Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 6 is implemented in relation to this skill.		
	Update/dispose	Practice APO07.03 activity 7 (Review training materials and programs on a regular basis to ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 7 is implemented in relation to this skill.		
B-8.5a	Understand good practice related to the **People, Skills and Competencies** and expected values. Assess the People, Skills and Competencies design, i.e., assess to what extent expected good practices are applied.				
	Good Practice	**Assessment Step**			
	Skill set and Competencies are defined.	• Determine that an inventory of Skills and Competencies is maintained by organizational unit, job function and individual. • Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organizational Structure, and by consequence, IT-related goals and enterprise goals. • Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities.			
	Skill levels are defined.	• Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and current Skill levels. • Assess the process for 360-degree performance evaluations.			
B-8.1 to B-8.5	Repeat steps B-8.1 through B-8.5 for all remaining **People, Skills and Competencies** in scope.				
	Repeat the steps described above for the remaining People, Skills and Competencies:				

IS Audit and Assurance Program—PCI DSS Compliance Program			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
People, Skills and Competencies			
Ref.	**Assurance Steps and Guidance**	**Issue Cross-reference**	**Comments**
	• Enterprise governance • Risk management proficiency • Customer service excellence • Security awareness training • PCI DSS framework, best practices and ancillary documentation proficiency • Information security testing and assessment • Information security experience • Network management experience • Change management experience • Development and implementation of compliance frameworks experience		

IS Audit and Assurance Program—PCI DSS Compliance Program		
Phase C—Communicate the Results of the Assessment		
Ref.	**Assurance Step**	**Guidance**
C-1	**Document exceptions and gaps.**	
C-1.1	Understand and document weaknesses and their impact on the achievement of enabler goals.	• Illustrate the impact of enabler failures or weaknesses with numbers and scenarios of errors, inefficiencies and misuse. • Clarify vulnerabilities, threats and missed opportunities that are likely to occur if enablers do not perform effectively.
C-1.2	Understand and document weaknesses and their impact on enterprise goals.	• Illustrate what the weaknesses would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources). Relate the impact of not achieving the enabler goals to actual cases in the same industry and leverage industry benchmarks. • Document the impact of actual enabler weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc. • Point out the consequence of noncompliance with regulatory requirements and contractual agreements. • Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, and cost).
C-2	**Communicate the work performed and findings.**	
C-2.1	Communicate the work performed.	• Communicate regularly to the stakeholders identified in A-1 on progress of the work performed.
C-2.2	Communicate preliminary findings to the assurance engagement stakeholders defined in A-1.	• Document the impact (i.e., customer and financial impact) of errors that could have been caught by effective enablers. • Measure and document the impact of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by enabler weaknesses. • Measure the actual business benefits and illustrate cost savings of effective enablers after the fact. • Use benchmarking and survey results to compare the enterprise's performance with others. • Use extensive graphics to illustrate the issues. • Inform the person responsible for the assurance activity about the preliminary findings and verify his/her correct understanding of those findings.
C-2.3	Deliver a report (aligned with the terms of reference, scope and agreed-on reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.	