
PCI
Security
Standards Council
PCI Security
Program Design
Bridging Theory and Practice
By Ciske van Oosten
Verizon Cyber Security Consulting

Speaker:

Ciske van Oosten

Ciske van Oosten
Head of Global Business Intelligence
Author of the Payment Security Report (PSR)

Verizon Cyber Security Consulting

verizon

PCI Security Standards Council

Agenda

Improving the Design of Your PCI Security Program

Insights based on 20 years of security program design and evaluation.

1. Common program design mistakes.
2. Measuring security program success.
3. The importance of a sensible program goal.
4. How to identify and overcome the most important program constraints.

PCI Security Standards Council

Designing and Managing Your PCI DSS v4.0 Transition Strategy

Q2 2022		H2 2022		H1 2023		H2 2023		H1 2024
Interpretation of the Standard	>	Resource Req Assessment	>	Gap assessment	>	Preassessment	>	Formal assessment

1. Interpretation of the PCI DSS v4.0

Clarification of goals and objectives, outcomes and expectations

2. Resource Requirement Assessment

An integrated analysis of the scope, requirements and constraints

3. Gap assessment

Pinpointing the exact difference (gap) between your current environment versus PCI DSS v4.0 requirements (present reality versus future reality)

4. Preassessment

A sampled review of compliance evidence and preparedness to determine readiness for the formal PCI DSS v4.0 validation assessment

5. Formal DSS v4.0 validation assessment

PCI Security Standards Council

Program Design & Performance

Expectations vs Reality

Expectations vs Reality

PCI Security Program Design & Performance

EXPECTATIONS	REALITY IN PRACTICE
1. The annual PCI DSS validation assessment will succeed the first time	1. Few organizations pass their annual validation assessment the first time - multiple requirements are usually not in place
2. The work assignment of the compliance team results in the right work being done, and to be completed in time	2. Assigned program tasks often do not contribute toward the program goal (lack of focus)
3. Program participants aim to achieve the same overall goal and objectives	3. An articulated PCI security goal statement is seldom communicated – no shared view of program objectives and requirements
4. The team knows how to design a program to be economical and to achieve results quicker (agile) – “doing more with less”	4. Insufficient attention to program design and methods to achieve effectiveness and efficiency
5. The team is capable of doing the work in the correct, logical order (critical path/chains)	5. Lacking project and program management skills

PCI Security Standards Council

Expectations vs Reality

PCI Security Program Design & Performance

EXPECTATIONS	REALITY IN PRACTICE
6. The team knows how to define and execute the security and compliance strategy	6. PCI security strategies are usually poorly defined, not documented and poorly communicated
7. The requirements and success factors (necessary conditions) to sufficiently meet objectives are known and communicated	7. Success factors are usually only partially known and not sufficiently analyzed and communicated
8. The cause and effect relationships between processes, people, technology and documentation are understood	8. Teams are inefficient and experience delays in getting the right work done - because program design and management steps are skipped
9. Teams know how to identify which constraints are the most important	9. People work on constraints that are not important and which should not receive priority attention
10. Teams know how to remove or reduce constraints	10. Teams often lack a proven method for reducing and removing security program constraints

PCI Security Standards Council

Common Security Program Design Mistakes

1. **No design**
   The security program is not well-structured. The relationships between program elements are not sufficiently known, undocumented and not communicated. A disorderly approach.

2. **Insufficient design**
   Inadequate focus - the program management scope is either too broad or has too narrow scope. Trial-and-error approach. Lack of structured implementation methods (what vs “how to”)

3. **Outcomes are not effective**
   Insufficient incorporation of “effectiveness” as a required outcome of controls and the environment.

4. **Inefficient program execution**
   Dependencies: deficient management of critical paths and critical chains. Sub-optimization.

5. **Unsustainable performance**
   Compliance management is a marathon, not a sprint. Ongoing constraint management is not built-in.

PCI Security Standards Council

Program Design & Performance

Measuring Program Success

Quotable Quotations

“It is not the daily increase but the **daily decrease**.
Hack away at the unessential.”

- Bruce Lee

“One reason so few of us achieve what we truly want is that we never **direct our focus**; we never concentrate our power.”

— Tony Robbins

“Tell me how you will **measure me**,
and then I will tell you how I will behave.
If you measure me in an illogical way,
don’t complain about illogical behaviour.”

— Eli Goldratt

Essential PCI Security Program Design Outcomes

1. An effective program	• **Get the right work done** – contributing to the achievement of the goal • **Evidence of assurance** that its control environment and requirements effectively meet the intent of the control objectives.
2. Strategically aligned	• Programs that supports **business objectives and strategy**. • Program design and execution are neither tactical nor reactive
3. Efficiently executed and economical	• **Produce economical program results** • Program is executed in a better manner - with minimum waste of resources • The capability to achieve more with less (despite scarcity of resources)
4. Sustainable performance	• **Integrated life cycle management** • The ability to sustain performance over extended periods without significant deviations. Rapid detection and correction of deviations.
5. Ongoing capability improvement	• Program includes ongoing **capability measurement and reporting**

The Goal of PCI Data Security

"The organization goal of a PCI security compliance program is to develop, maintain and continuously improve a mature control environment that offers reasonable assurance for the effective, ongoing security of payment card data in a consistent, predictable and sustainable manner.

To achieve this goal, the PCI security compliance program is integrated with and supported by additional security, risk management and governance frameworks, a security operating model, a strategy and a security business model."

—Verizon 2022 Payment Security Report

"The ongoing effective security of payment account data."

The goal that all PCI security programs should aim to achieve includes the following 5 criteria:

1. Developing, maintaining and continuously improving
2. a mature control environment
3. that offers reasonable assurance for
4. the effective, ongoing security of payment card data
5. in a consistent, predictable and sustainable manner.

The Constraints of Organizational Proficiency “the 7 Cs”

A categorization of common limitations that restricts or prevents program performance improvement

1. Capacity

Limitations on the amount of resources that can be allocated to security and compliance

2. Competence

The level of experience and skill at an individual level to support security and compliance

3. Capability

The level of proficiency at team and organization levels – what people can achieve collectively

4. Commitment

The pledge from stakeholders to undertake the actions needed to achieve the security goals

5. Communication

The frequency and quality with which participants exchange information

6. Culture

The sum of an organization’s attitudes, actions and behaviors toward security and compliance

7. Cost

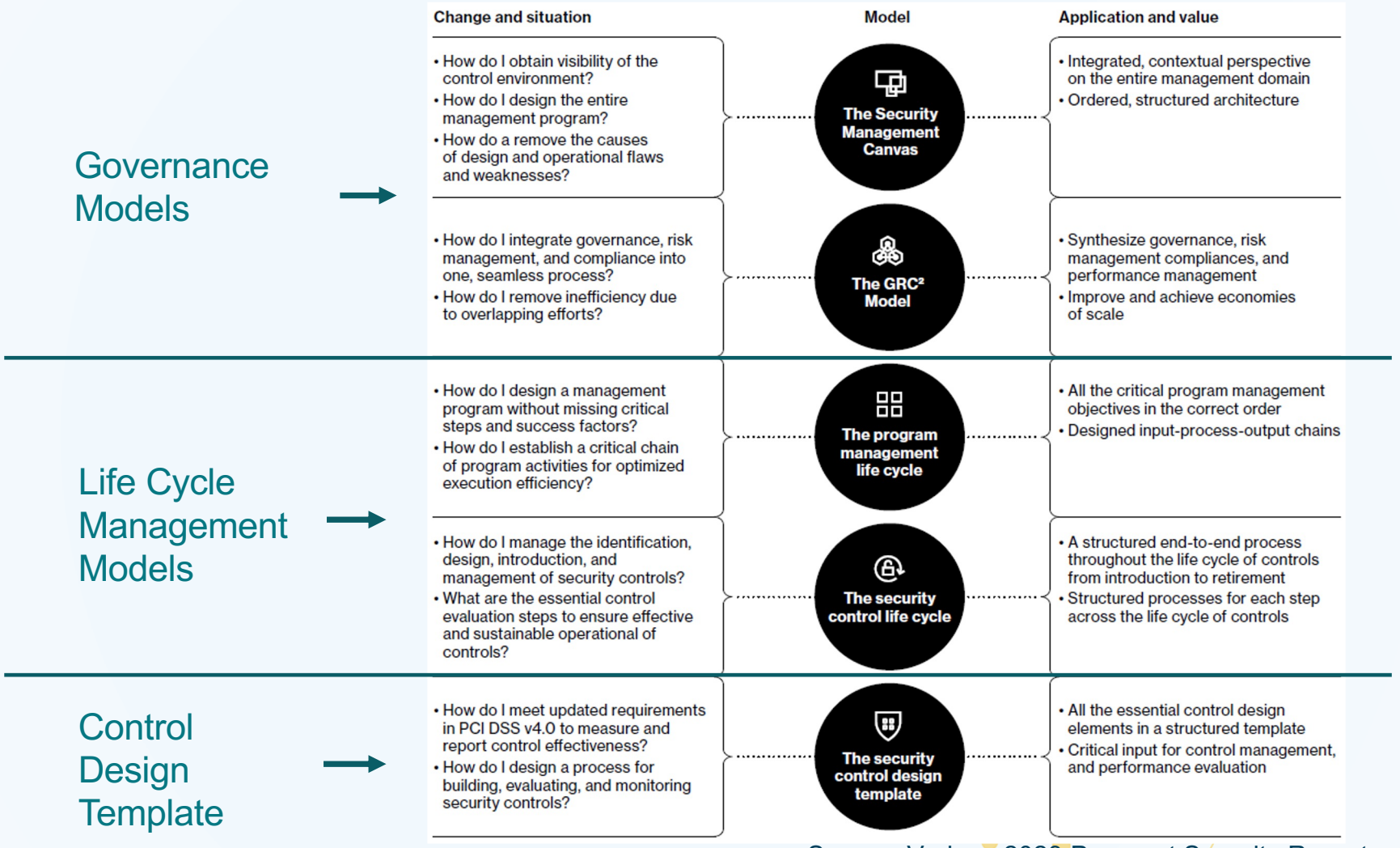
The amount of time and money allocated and required to achieve objectives and goals

PCI Security Standards Council

Program Design & Performance

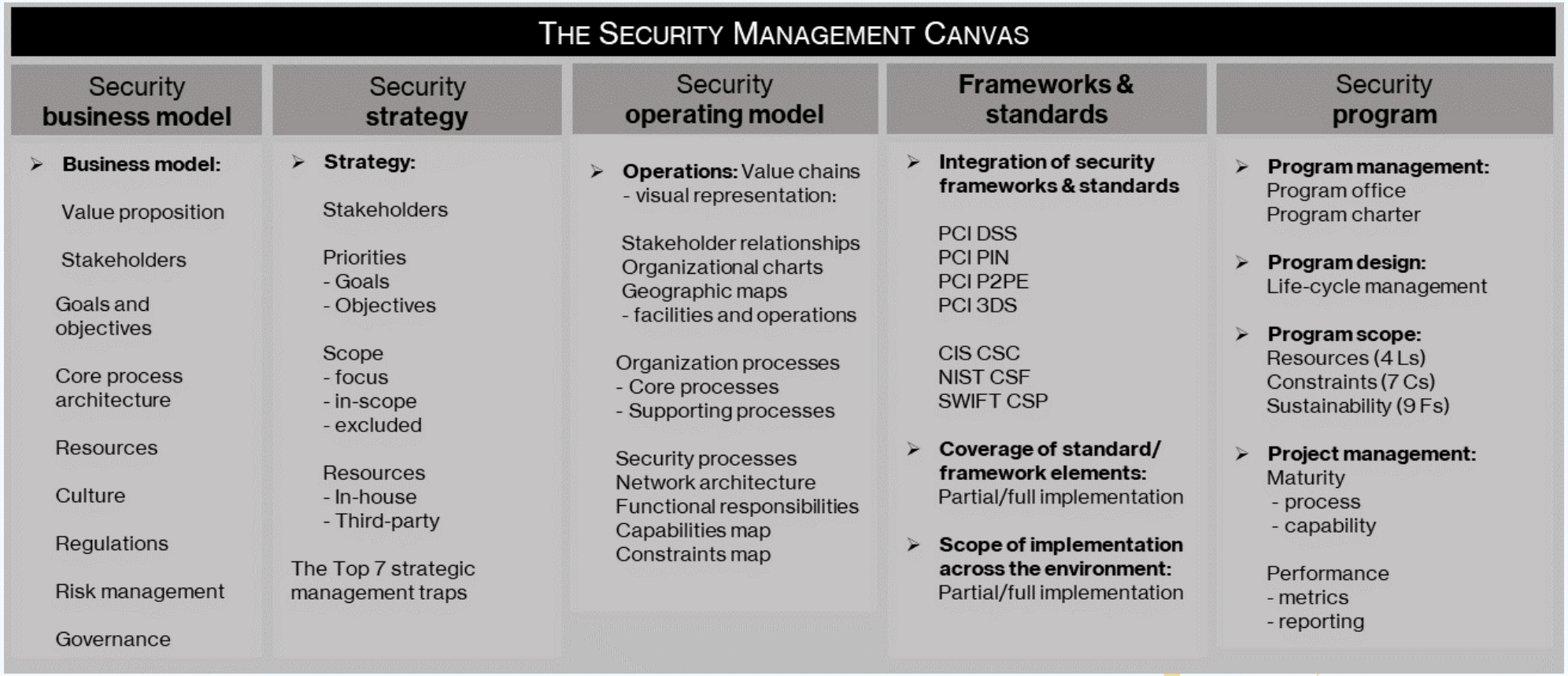
Management Models

Integrated Security Program Design Models and Methods



Source: Verizon 2023 Payment Security Report

The Security Management Canvas



Source: Verizon 2023 Payment Security Report

The GRC$_2$ Model

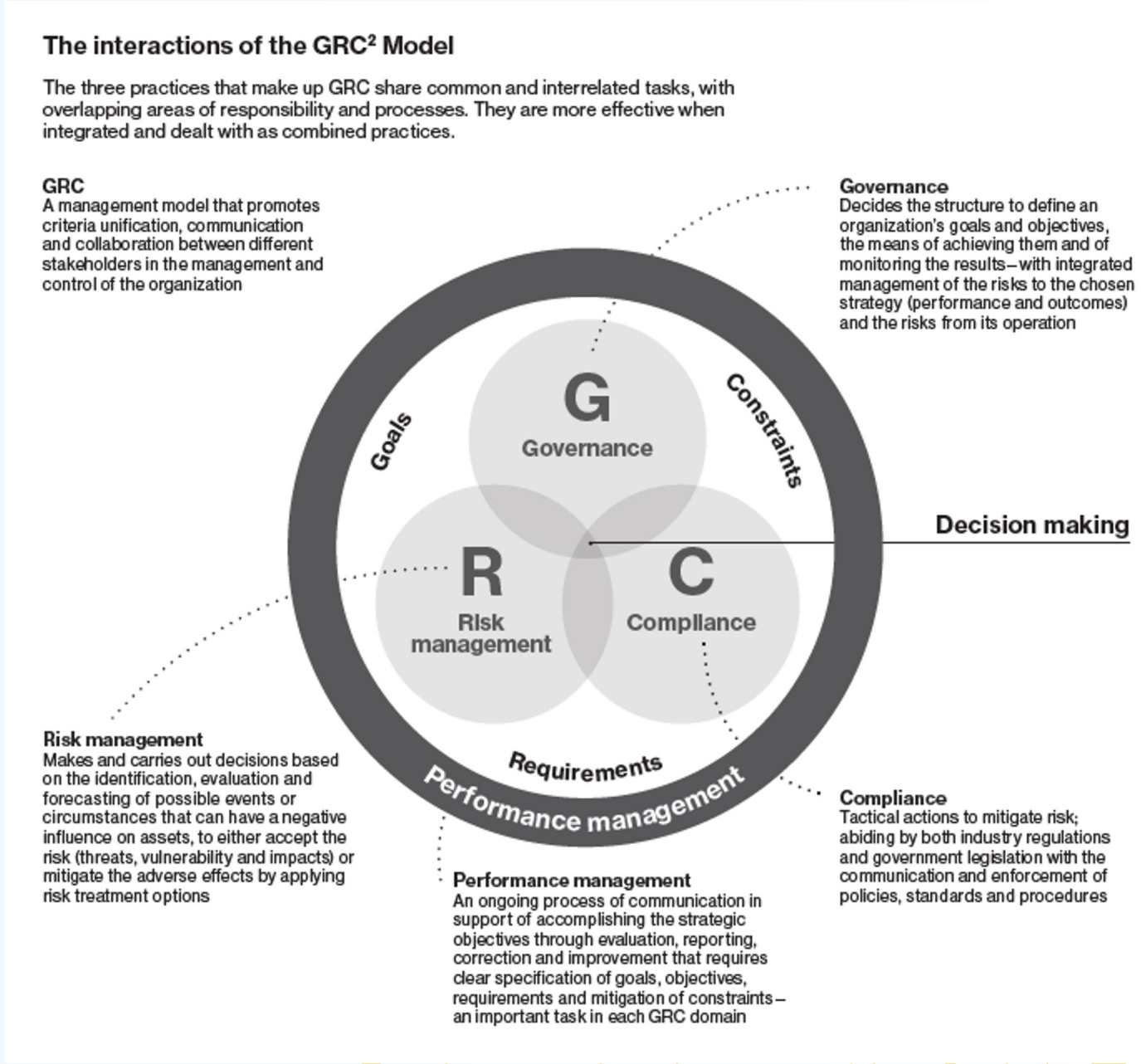
A unified approach to integrate overlapping decision-making and performance management of:

1. **G**overnance,
2. **R**isk Management, and
3. **C**ompliance programs.

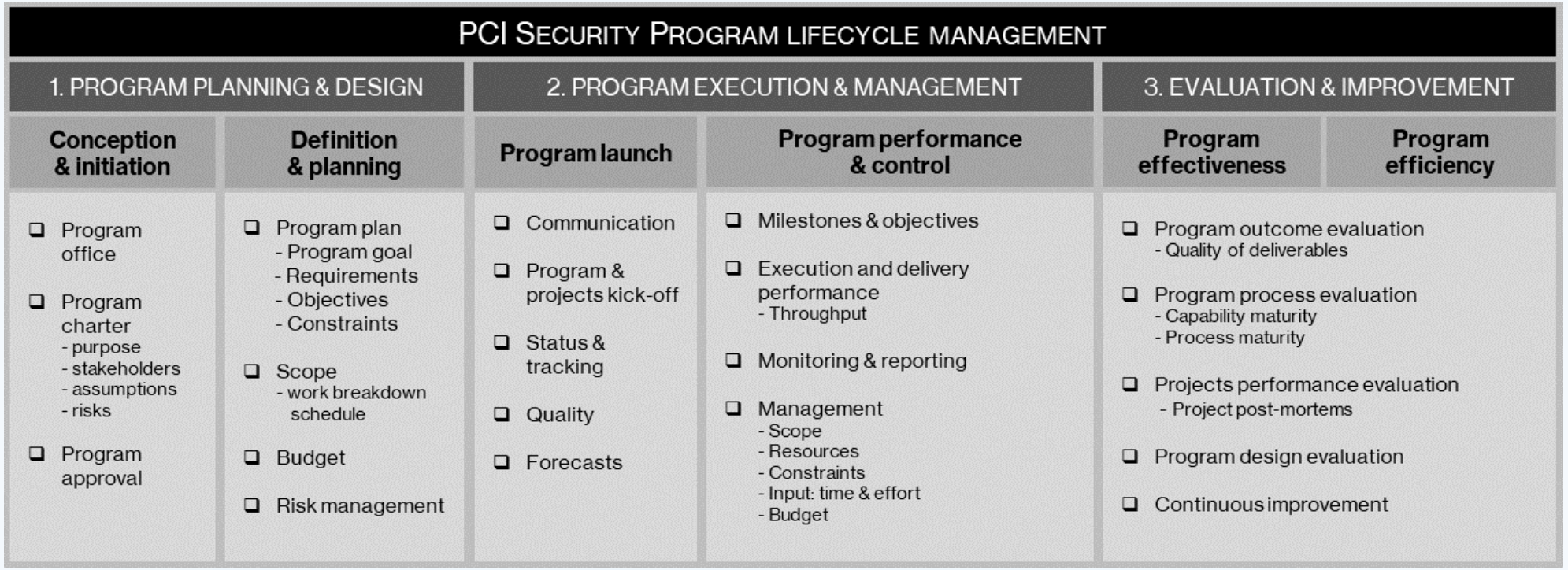
with a model to structure the definition, evaluation and alignment of:

1. the **G**oals,
2. the **R**equirements, and
3. the **C**onstraints

of all three domains.



Security Program Life Cycle Management



PCI Security Program Lifecycle Management

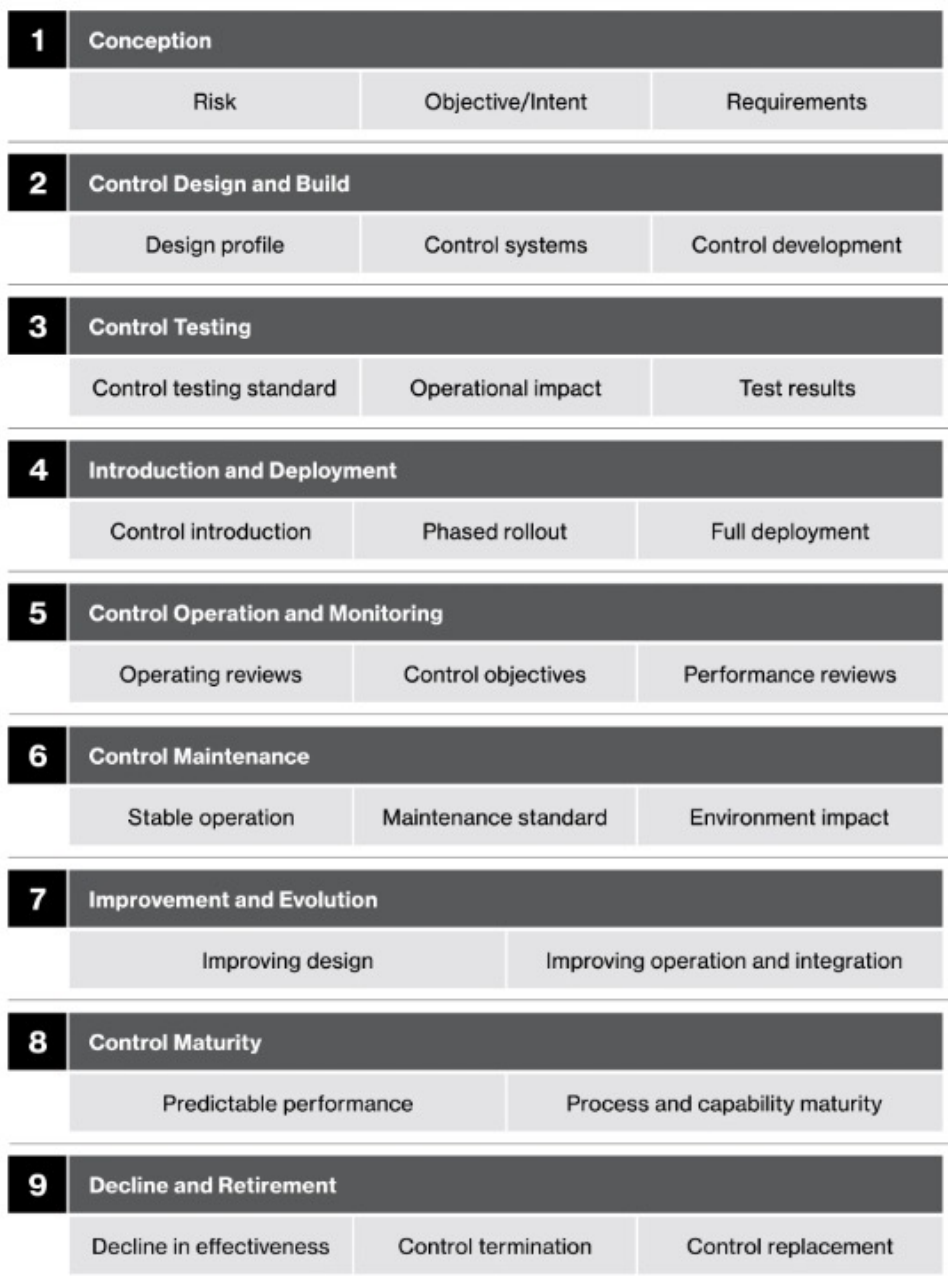
1. Program Planning & Design		2. Program Execution & Management		3. Evaluation & Improvement	
Conception & initiation	**Definition & planning**	**Program launch**	**Program performance & control**	**Program effectiveness**	**Program efficiency**
❑ Program office ❑ Program charter - purpose - stakeholders - assumptions - risks ❑ Program approval	❑ Program plan - Program goal - Requirements - Objectives - Constraints ❑ Scope - work breakdown schedule ❑ Budget ❑ Risk management	❑ Communication ❑ Program & projects kick-off ❑ Status & tracking ❑ Quality ❑ Forecasts	❑ Milestones & objectives ❑ Execution and delivery performance - Throughput ❑ Monitoring & reporting ❑ Management - Scope - Resources - Constraints - Input: time & effort - Budget	❑ Program outcome evaluation - Quality of deliverables ❑ Program process evaluation - Capability maturity - Process maturity ❑ Projects performance evaluation - Project post-mortems ❑ Program design evaluation ❑ Continuous improvement	

Source: Verizon 2023 Payment Security Report

The Security Control Life Cycle

Security programs should include management of controls through each stage of its life cycle:

1. Conception
2. Control design and build
3. Control testing
4. Introduction and deployment
5. Control operation and monitoring
6. Control maintenance
7. Improvement and evolution
8. Control maturity
9. Control decline and retirement



Source: Verizon 2023 Payment Security Report

Security Control Design Profile/Template

1. Control objective	Defines the applicable control objective(s) of the control or control system
2. Control owner	Assigns ownership and responsibilities
3. Control function	Describes the control function, such as management, procedural or technical
4. Control type(s)	Describes the control types, such as preventative, detective, corrective or directive
5. Architecture	Defines the control architecture, such as system-specific, common or hybrid
6. Control risk	Describes key risks that the control mitigates; control-to-risk matrix or mapping
7. Control testing	Describes or references control test procedures and standards
8. Implementation	Specifies implementation scope, control, procedure implementation and dependencies
9. Operation	Documents control operation specifications and defines scope processes, operational dependencies, supporting processes, and component impacts on people, systems, processes and third parties
10. Maintenance	Addresses control maintenance specifications, scope and maintenance processes
11. Performance metrics	Provides a list of key performance indicators (KPIs) and other metrics to measure performance
12. Governance	References related policies, standards, frameworks and regulations

Source: Verizon 2023 Payment Security Report

PCI Security Program Design

A Payment Security Report insights White paper

The Verizon 2023 Payment Security Report insights White paper

Title: Advanced PCI Security Program Management Design

Released: August 23rd, 2023

30 pages

Download: https://www.verizon.com/paymentsecurityreport

PCI Security Standards Council

An Effective Program Management Approach

A logical approach for solving complex challenges

1. **Purpose** before planning
(start with “why,” then formulate goals)

2. Clarity on **objectives**
(intermediate steps to achieve the goals)

3. **Requirements** for achieving objectives
(necessary and sufficient conditions)

4. **Constraints** analysis of requirements
(focus on removing the most significant limiting factor)

And now that you actually know what you are dealing with (scope and impact):

5. **Strategy** development & communication
(focused allocation of resources)

6. **Program** design and implementation
(program- and project-level execution of the strategy)

7. Continuous re-evaluation and **improvement**
(performance management)

Thank you!

PCI Security Standards Council®