

Maintaining Compliance



John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire www.withoutfire.com



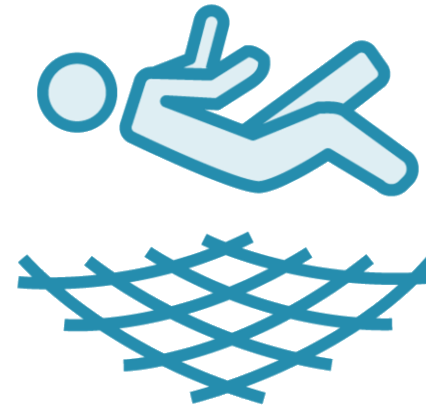
Why Bother?



You promised!



Criminals steal
payment card
data



Reduces breach
penalties



You have to do it
again in a year



Three Reasons Why Compliance Fails

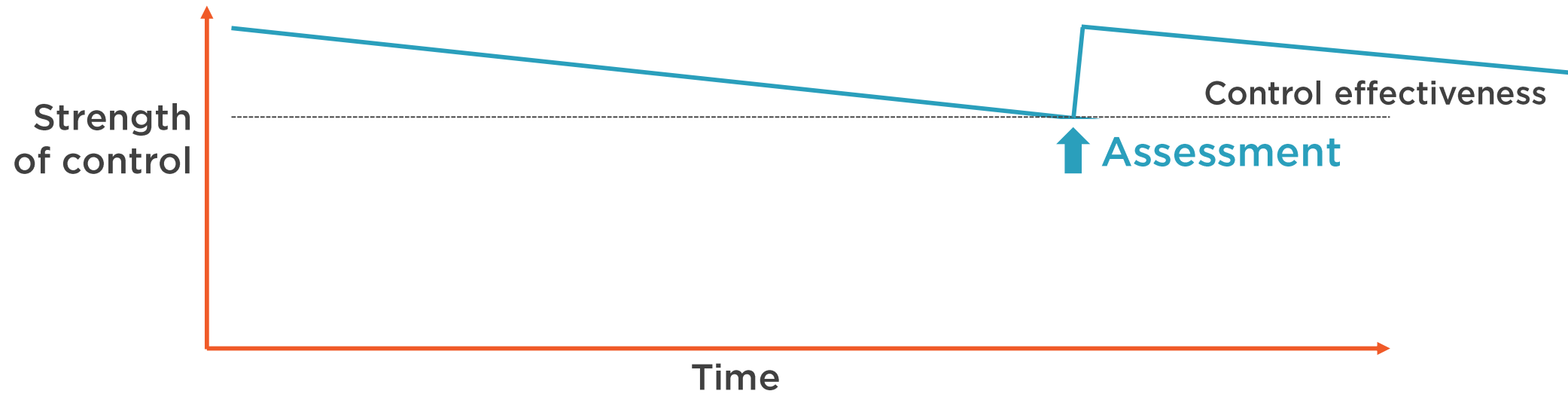
1. Control decay

**2. Scheduled
tasks ignored**

3. Change



Control Decay



Control Maturity Management Stops Decay



All controls (requirements) decay over time

Two ways of preventing this

- Optimism
- Management

Maturity Levels



1. Initial (chaotic)



2. Repeatable



3. Defined / Integrated



PCI DSS Gets you here



4. Managed



This is where control decay is prevented



5. Optimizing



Which Controls to Prioritize?



Those that give the largest
risk reduction

Those that tend to decay
more frequently



PCI DSS Requirements v3.2	Milestone					
	1	2	3	4	5	6
Requirement 1: Install and maintain a firewall configuration to protect cardholder data						
1.1 Establish and implement firewall and router configuration standards that include the following:						
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations						6
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1					
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	1					
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone		2				
1.1.5 Description of groups, roles, and responsibilities for management of network components						6
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.		2				
1.1.7 Requirement to review firewall and router rule sets at least every six months						6
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. <i>Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.</i>						
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.		2				
1.2.2 Secure and synchronize router configuration files.		2				
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.		2				
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.						

Prioritized Approach

Risk-categorization of requirements

https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2_1.pdf

1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	2
1.3.5 Permit only "established" connections into the network.	2



2019 Payment Security Report

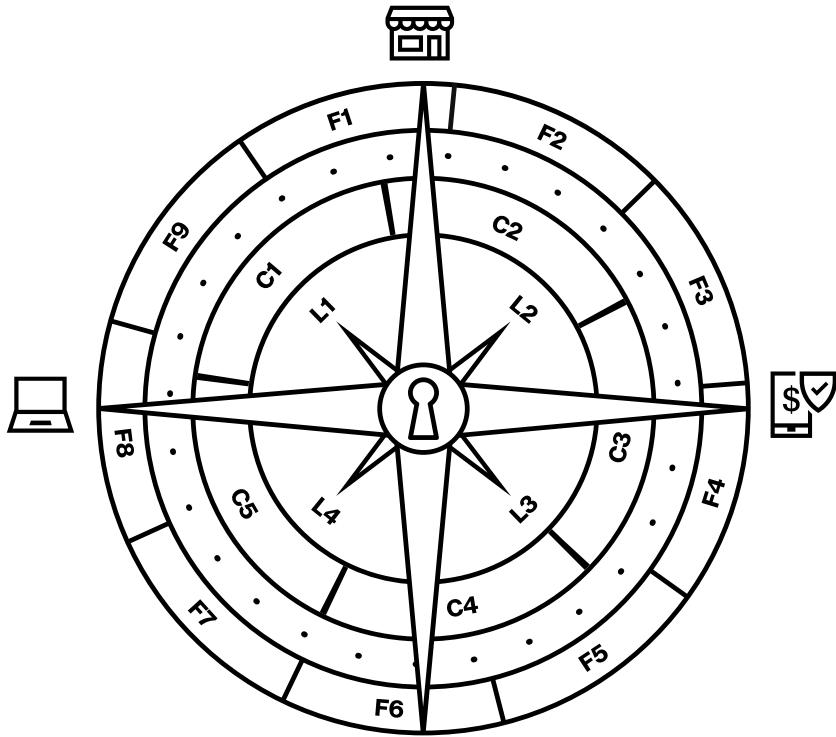
Published annually

Analysis of ongoing PCI DSS compliance

Where organizations 'fail' on second and subsequent assessments

- i.e. Where it is common to find control decay

Analysis of data breaches



<https://enterprise.verizon.com/resources/reports/2019-payment-security-fullreport-bl-global.pdf>

Decayed Requirements Most Likely to Be the Cause of a Data Breach *

1

**Network security
(typically segmentation)**

6

**Patching known vulnerabilities
Simple coding problems**

* 2019 Verizon Payment Security Report



Worst Maintained Controls *

11.2	Vulnerability scans
6.2	Patching
11.3.3	Remediate penetration test findings
1.1	Have and use firewalls properly
8.3	MFA for remote administration
8.1	Give users unique IDs and manage them
4.1	Encryption of data in transit (Bad SSL / TLS)
10.6	Examine logs to detect malicious activity

* 2019 Verizon Payment Security Report



Why Compliance Fails

1. Control decay

2. Scheduled
tasks ignored

3. Change



Prescriptive Scheduled Tasks

Daily
(every day)

Monthly
(every 30 days)

Quarterly
(every 90 days)

Six Monthly
(every 180 days)

Annually
(every 360 days)



Daily



10.6.1	Log review
10.6.3	Follow up exceptions and anomalies (includes 11.5.1)

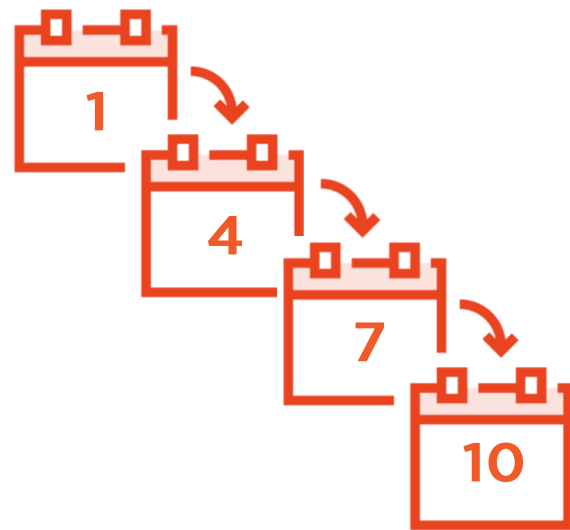
Monthly




6.1	Identification of security vulnerabilities
6.2	Management of patching

Not specified directly but ...

12.8.4	Monitor all service provider's compliance and obtain updated Attestations of Compliance
--------	---

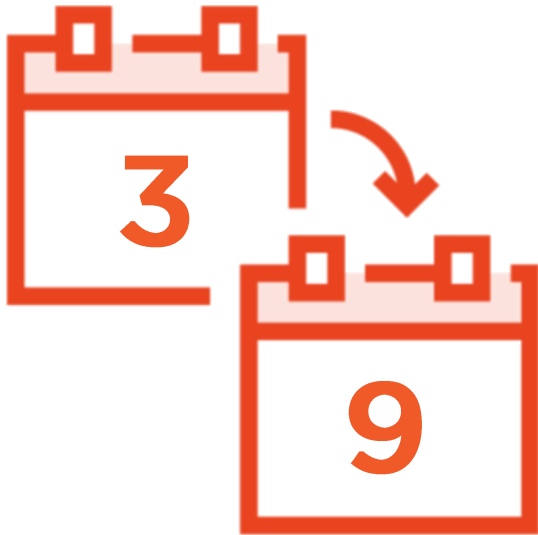


Quarterly

3.1	Deletion of cardholder data beyond retention period
8.1.4*	Remove/disable inactive accounts
11.1.1	Inventory of wireless access points
11.2.1	<u>Internal</u> vulnerability scans
11.2.1	Manage remediation of <u>internal</u> vulnerability scans
11.2.2	<u>External</u> ASV vulnerability scans
11.2.2	Manage remediation of <u>external</u> ASV vulnerability scans
	Send <u>external</u> ASV vulnerability scans to acquirer / card brand



Every Six Months



1.1.7 Review Firewall Rule Sets



Annually



6.5	Train developers
6.6	Web-facing application vulnerability assessment (if not using a WAF)
9.5.1	Review the security of locations of backup media
9.7.1	Annual inventory of physical media containing cardholder data



Annually



11.3.1	External penetration test
11.3.1	Internal penetration test
11.3.4	Segmentation penetration test
12.1.1	Review security policy
12.2	Risk assessment
12.6.1	Ensure all personnel with access to the CDE receive annual training ...
12.6.2	... and they acknowledge this
12.8.4	Review service providers*
12.10	Review and test incident response plan



Why Compliance Fails

1. Control decay

2. Scheduled
tasks ignored

3. Change





Business

- Payment Processes
- Locations
- Mergers, acquisitions

People

- Responsible for IT
- Responsible for PCI DSS
- Users

Technology

- Systems
- Networks
- Clouds



What Change Is Typically Significant?

New additions

**Upgrades
(hardware & software)**

**Cardholder
data flows**

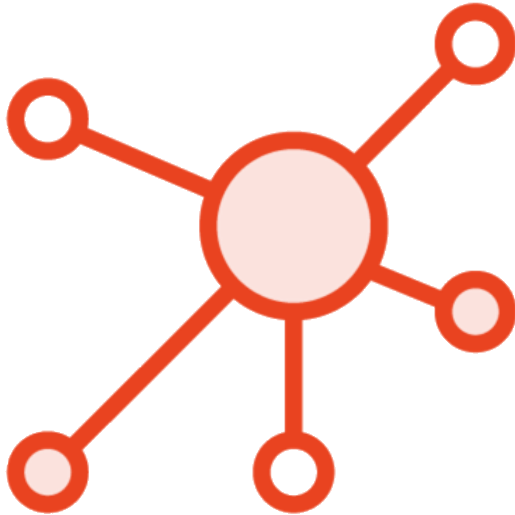
**Boundary
of the CDE**

**Supporting
infrastructure**

**Third party
service providers**



Network Changes



1.1.1	Approval of change
1.1.1	Documentation that <u>test</u> of change took place afterwards
1.1.2	Update network diagram
1.1.3	Update cardholder data flows (if affected)
1.1.6	Update permitted protocols if new protocol /service added
If significant change	
11.2	Vulnerability scans (Intl / Extnl)
11.3	Penetration tests (Intl / Extnl)

If significant change



Changes to Build Standards



2.2 Approval of change

If significant change

11.2 Vulnerability scans (Intl / Extnl)

11.3 Penetration tests (Intl / Extnl)



Changes to Data Retention Policies



3.1 Approval of change



Cryptographic Key Changes



3.6	Decision to change keys (why)
3.6	Approval of decision to change encryption keys
3.6	Supervision and documentation of key ceremony
3.6.8	Update key custodian register on change of roles
3.6.8	Maintain written key custodian acknowledgements



Change Management



6.4.5	Approval and classification of change (major / minor)
6.4.5	Validation that change management documentation complies with 6.4.5



Changes to Access Management



7.1.4 Approval of changes to access management (ie new groups and access rights within the CDE)

8.1.2 Approval of new users in the CDE



Changes to Media Access



- | | |
|--------------|---|
| 9.6.3 | Approval of access to physical media containing cardholder data |
| 9.7.1 | Update & Maintain media log when the physical media containing cardholder data is accessed |



People-related Changes



3.6.8	Update key custodian register on change of roles and signed acknowledgements
8.1.2	Starters (joiners), movers, leavers
12.6.1	Training and screening
12.7	Training of new users
12.5	Are there still people in roles with 12.5 responsibilities assigned?



Changes to Service Providers

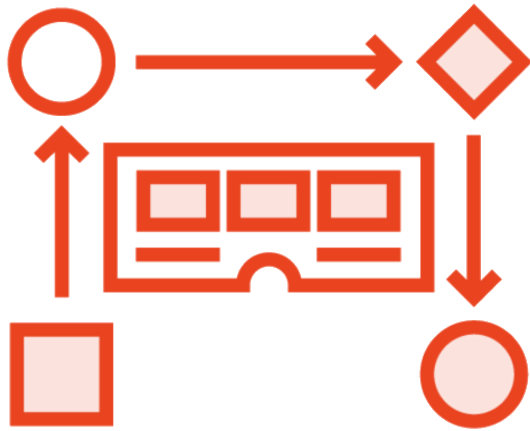


12.8.1 Update service provider register

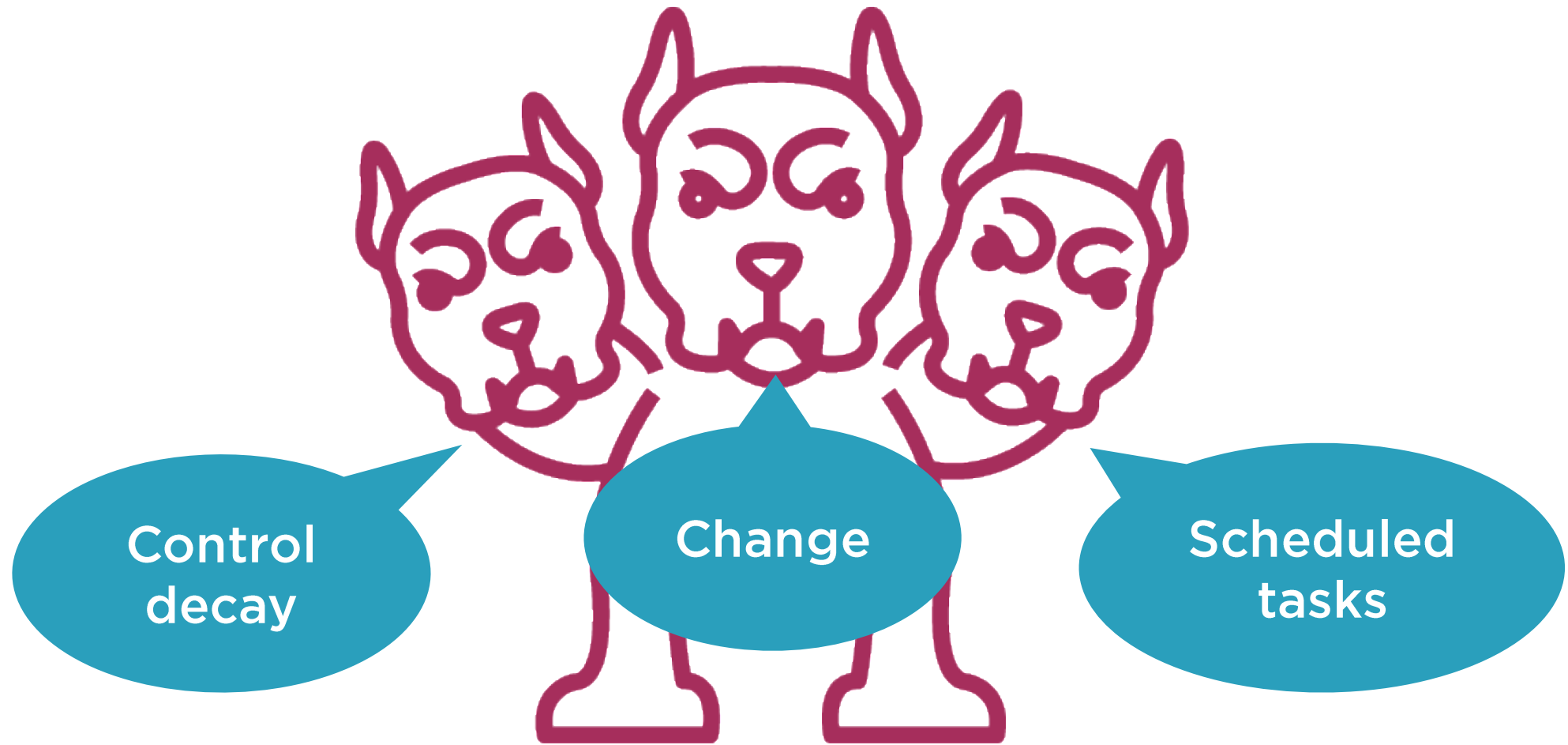
12.8.3 Follow documented process to engage new service providers



Significant Business Change



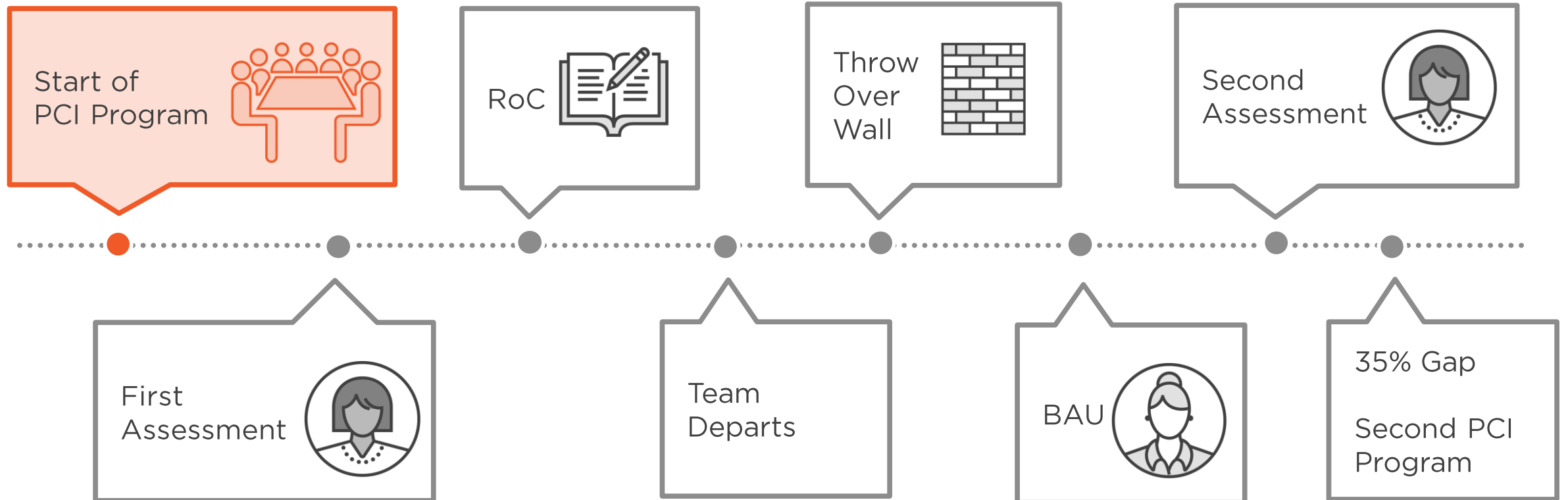
12.1.1	Review security policy
12.2	New risk assessment
12.5	Update responsibilities in the event of a business restructure (12.5 responsibilities are role not person based)
12.10	Review incident response plan*



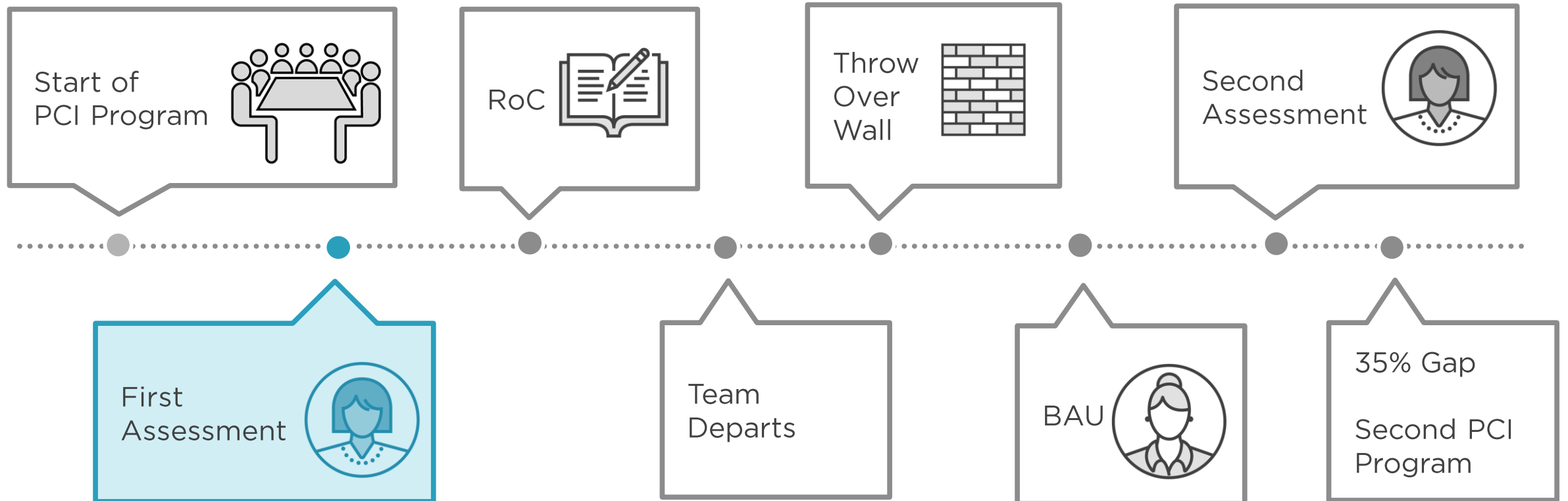
Embedding BAU Must Be Part of a Program



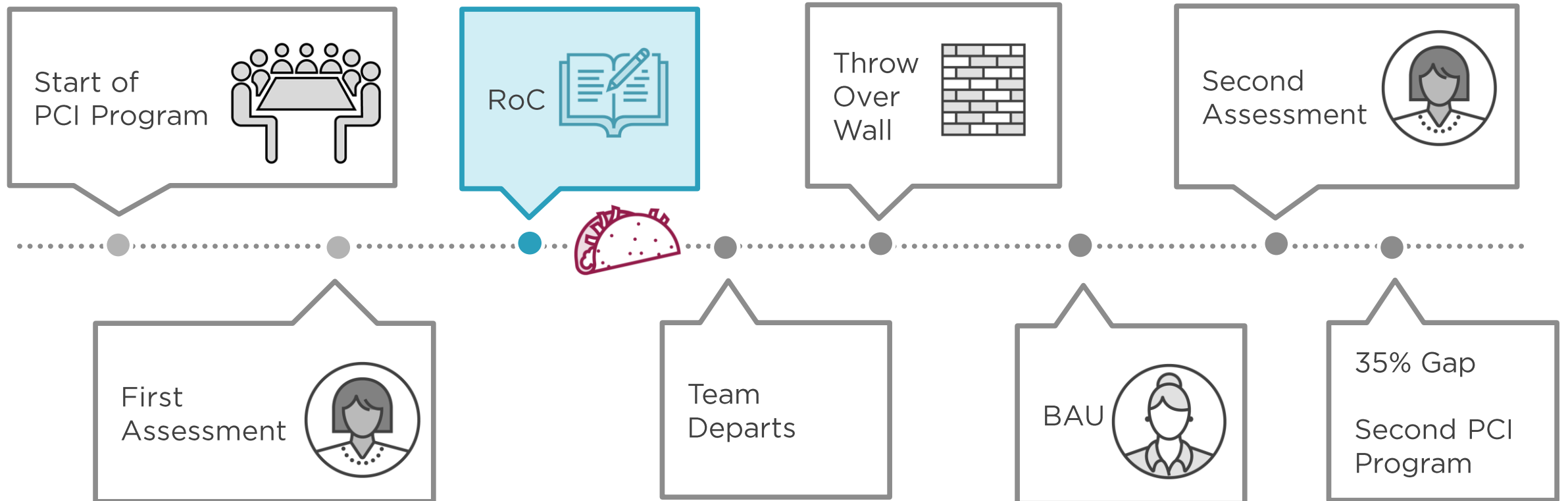
Typical Timeline



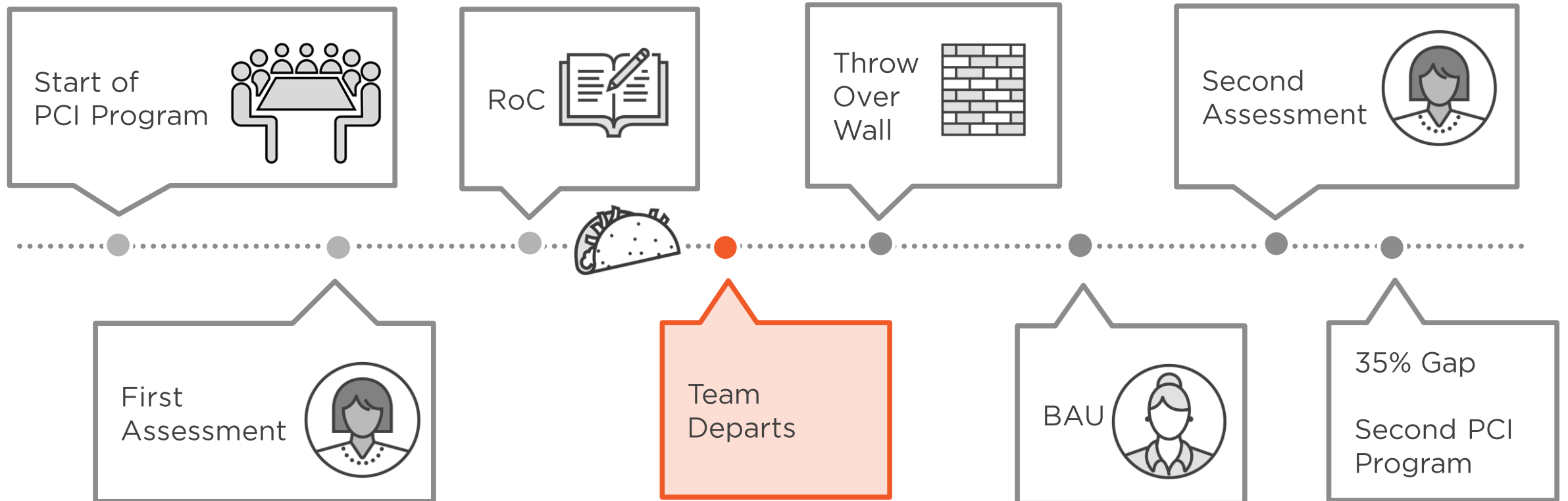
Typical Timeline



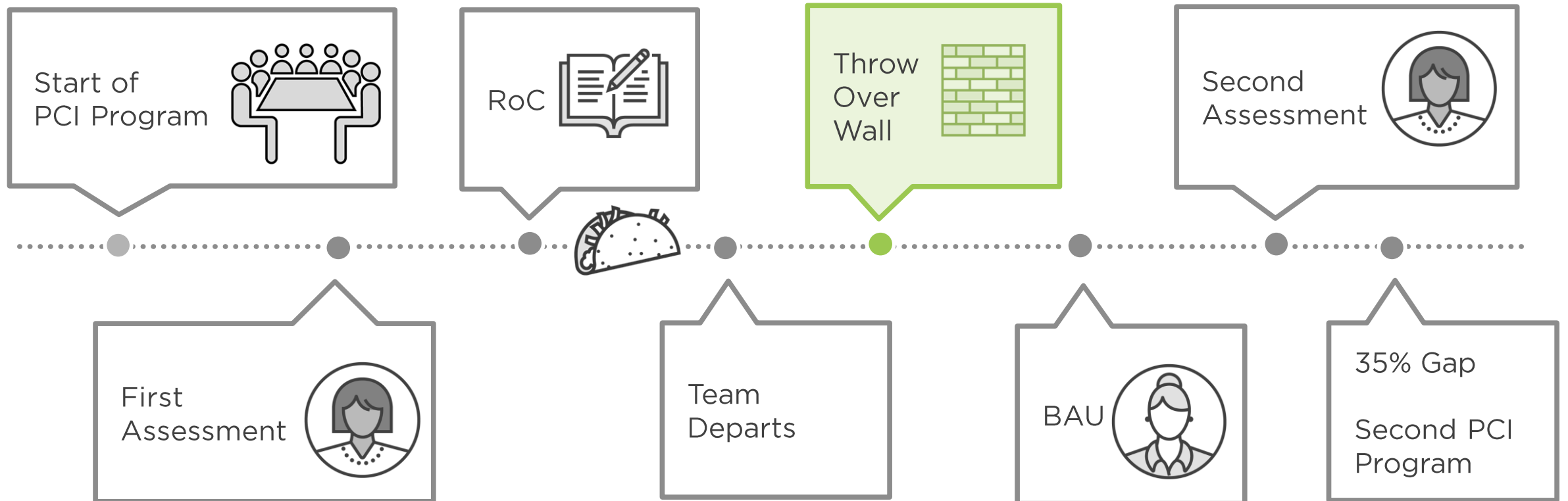
Typical Timeline



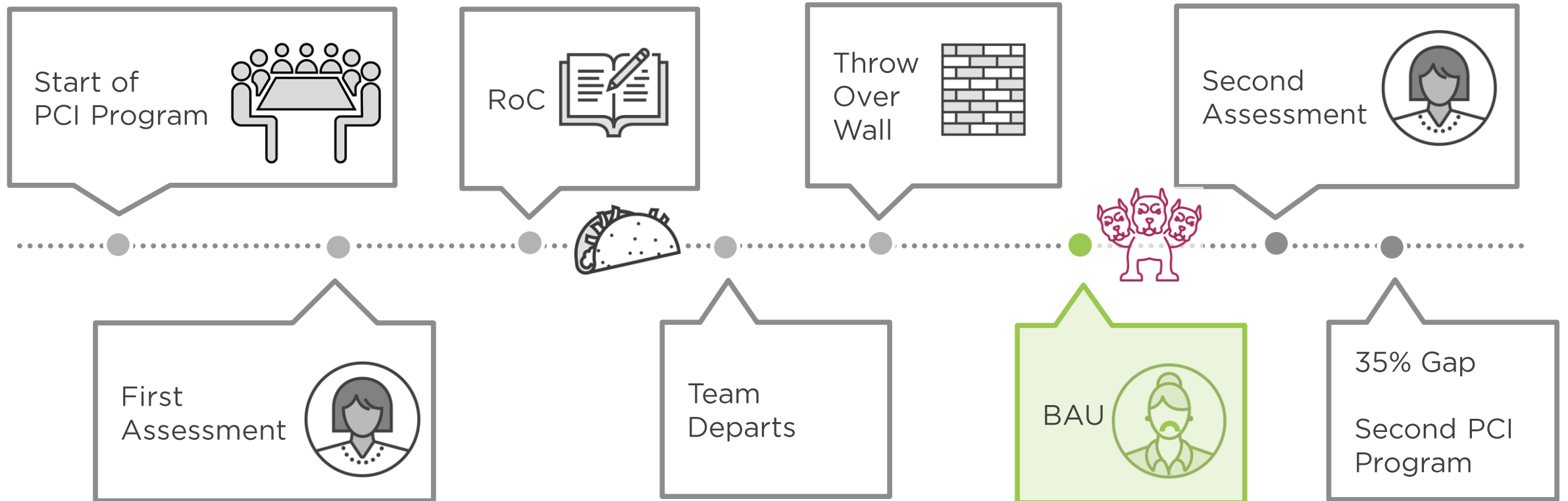
Typical Timeline



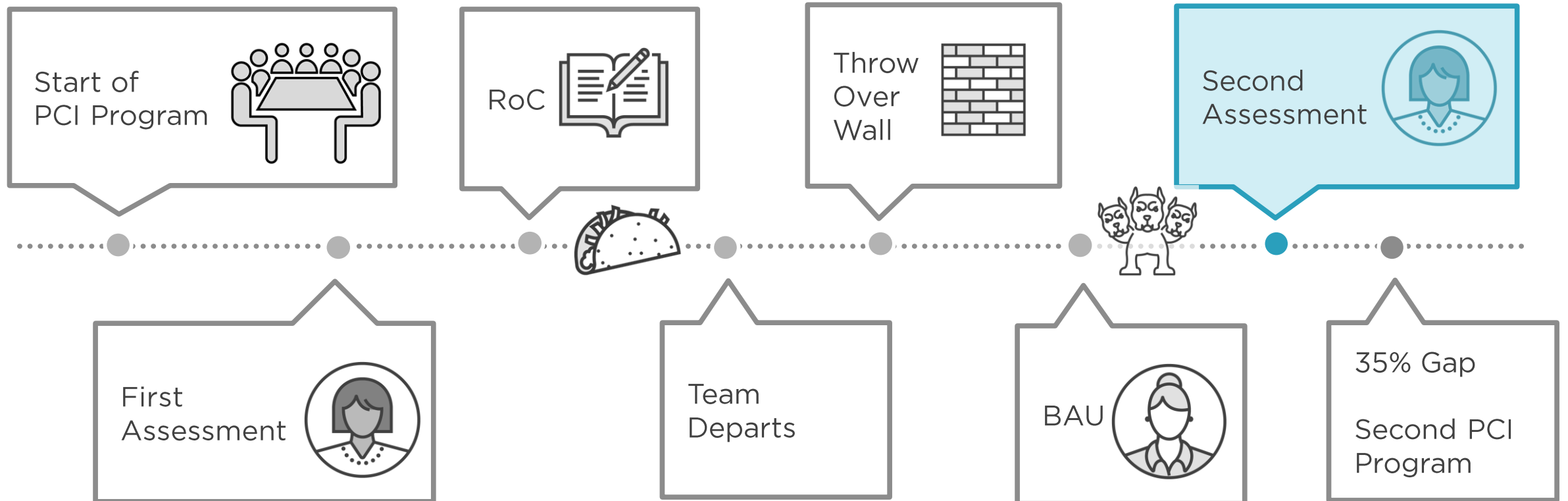
Typical Timeline



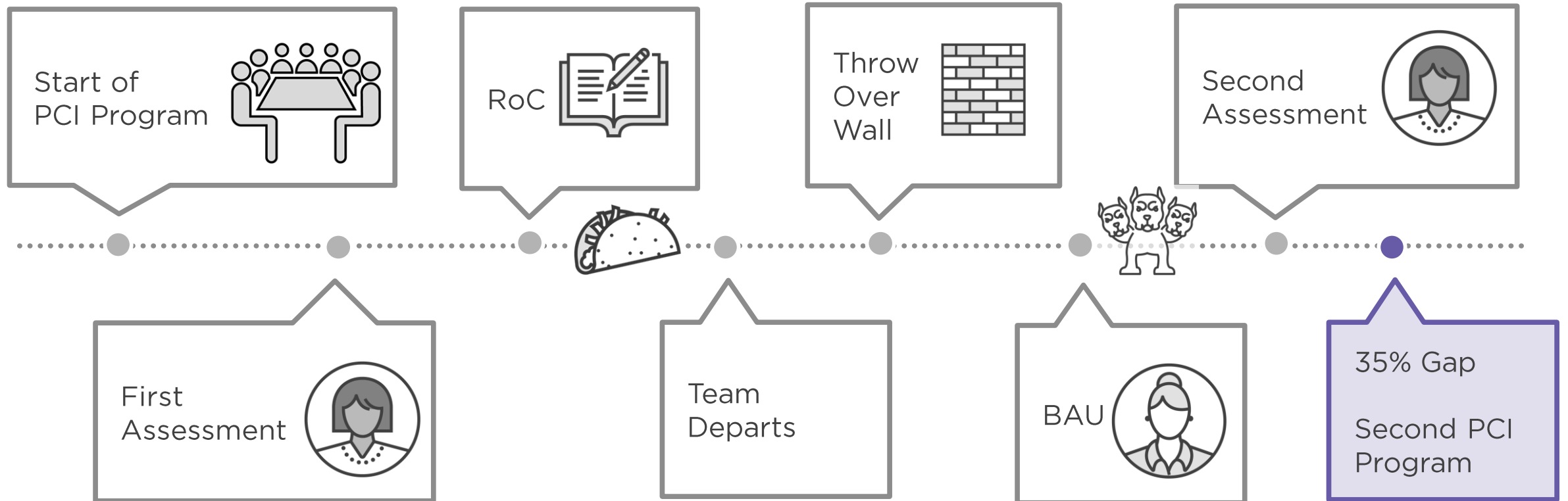
Typical Timeline



Typical Timeline



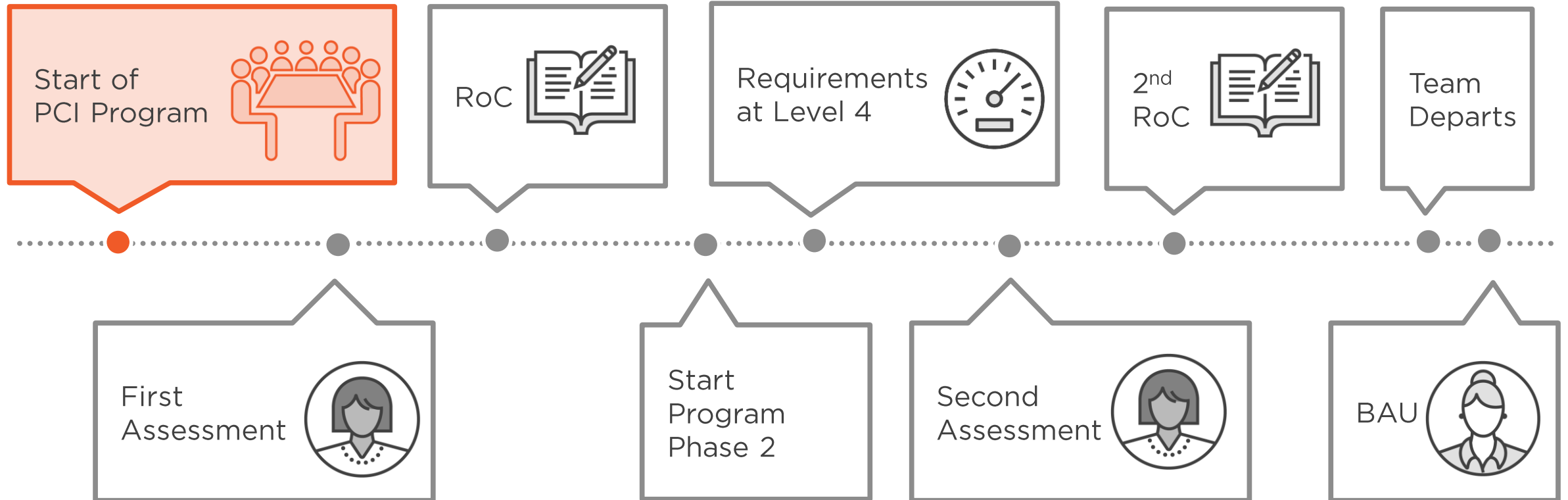
Typical Timeline



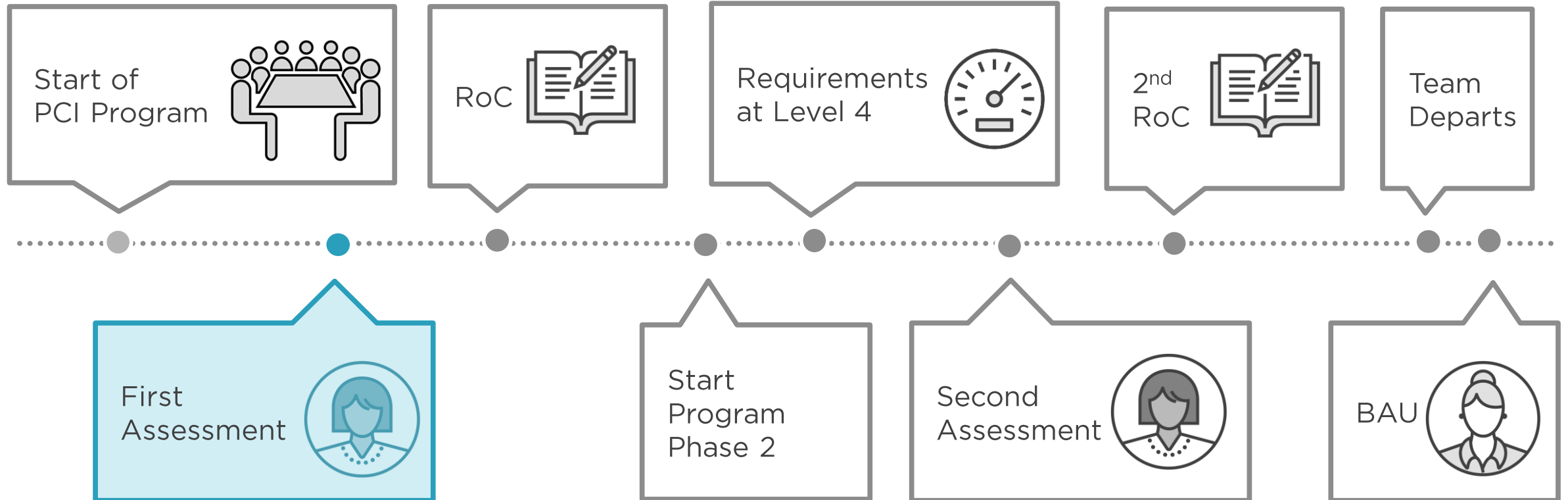
There Is a Better Way



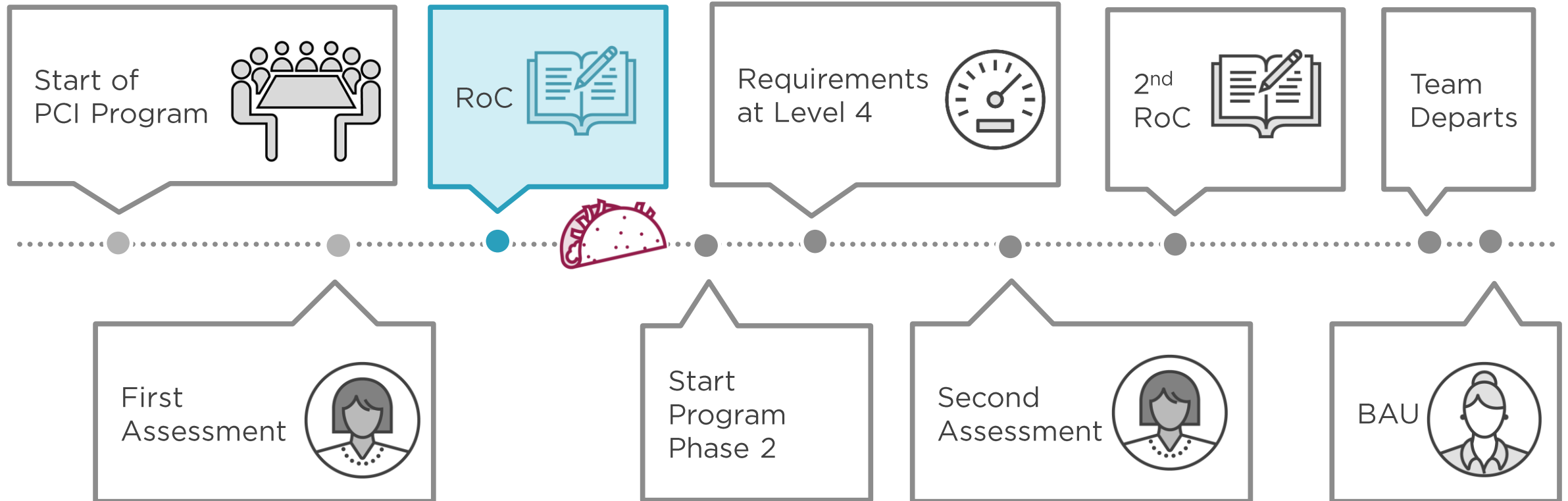
A Better Approach



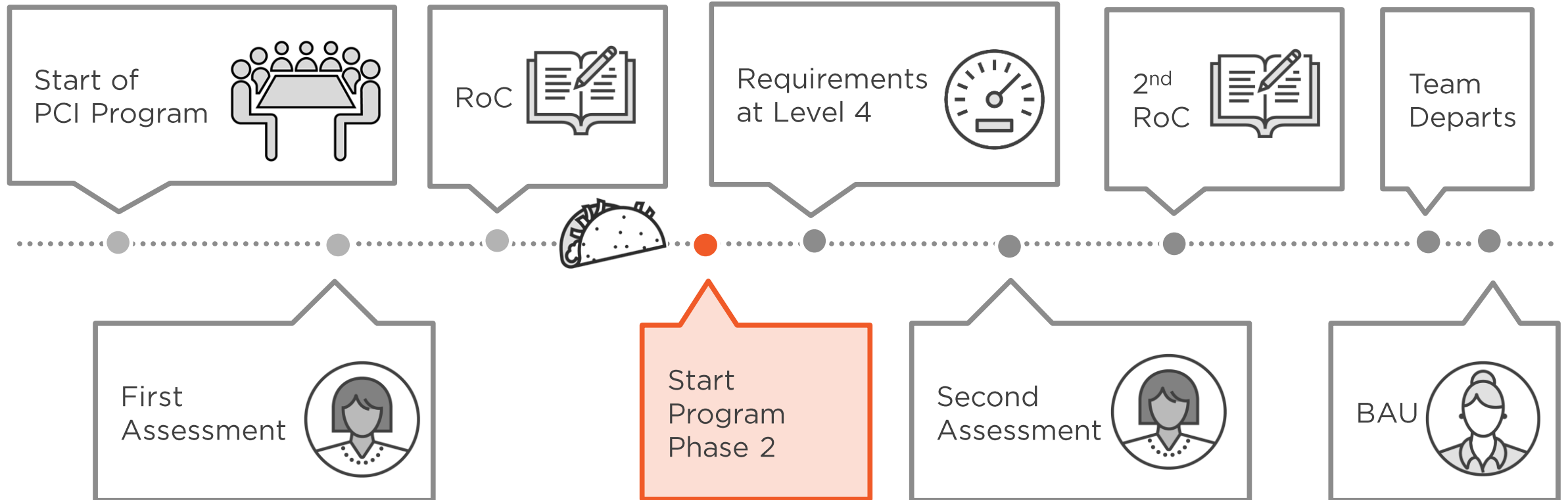
A Better Approach



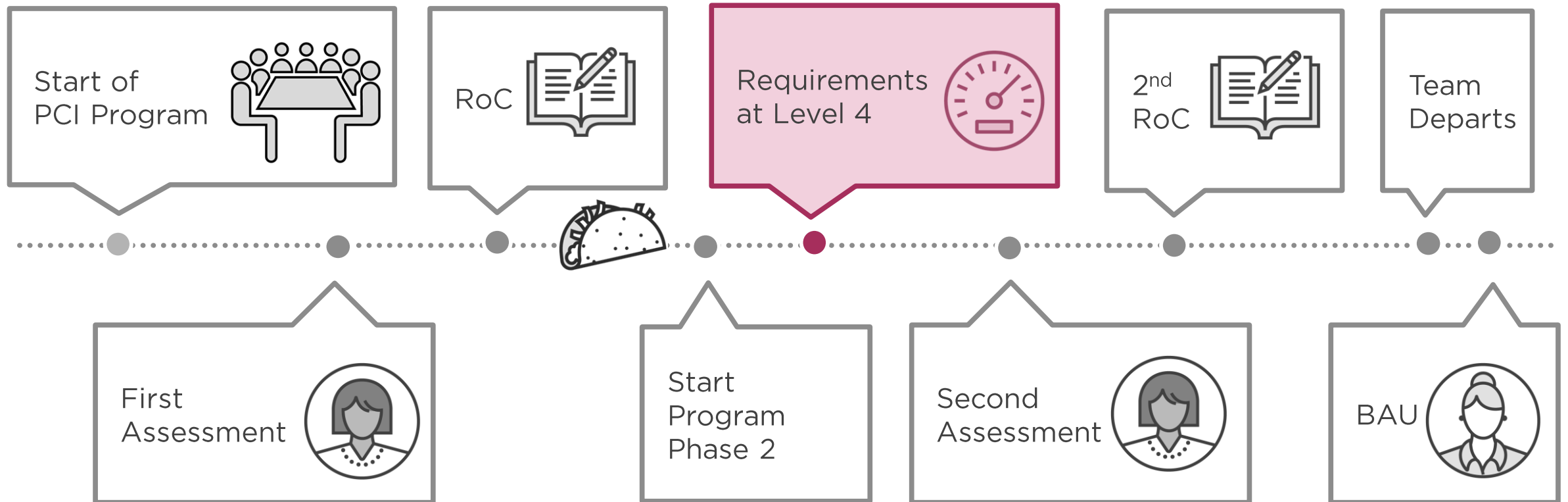
A Better Approach



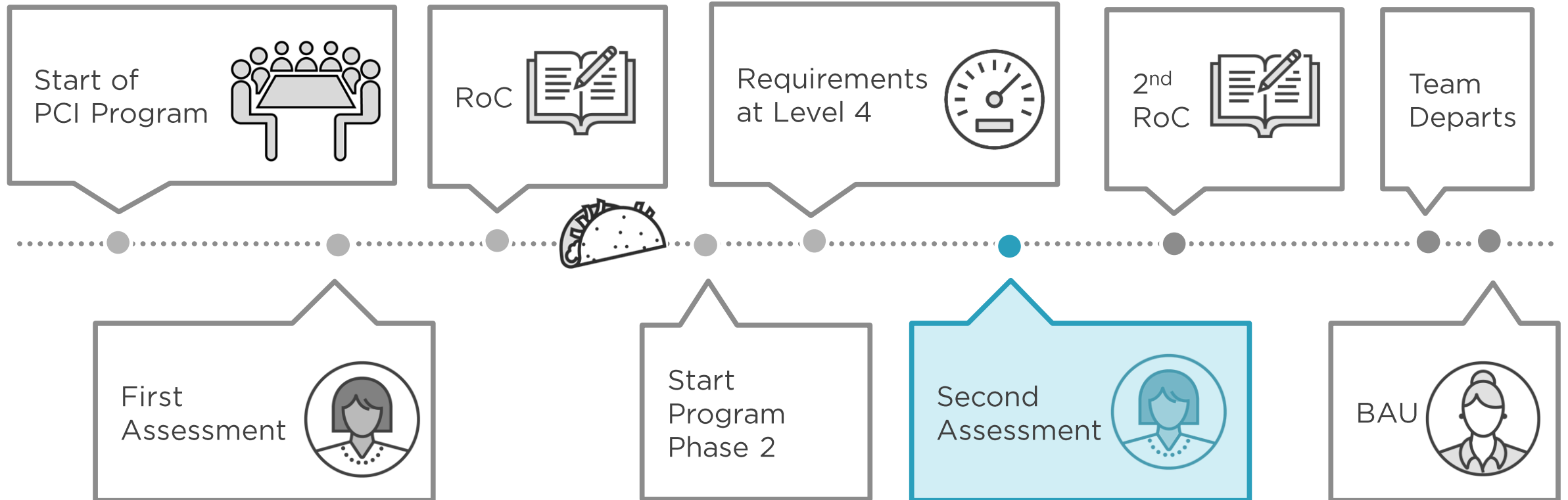
A Better Approach



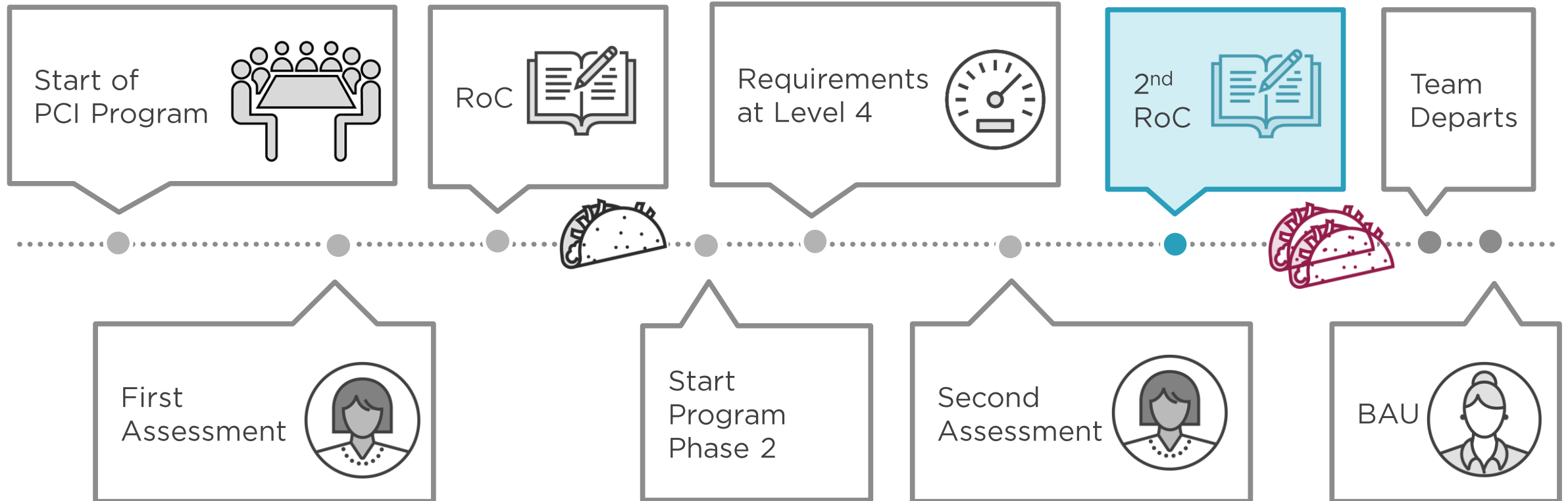
A Better Approach



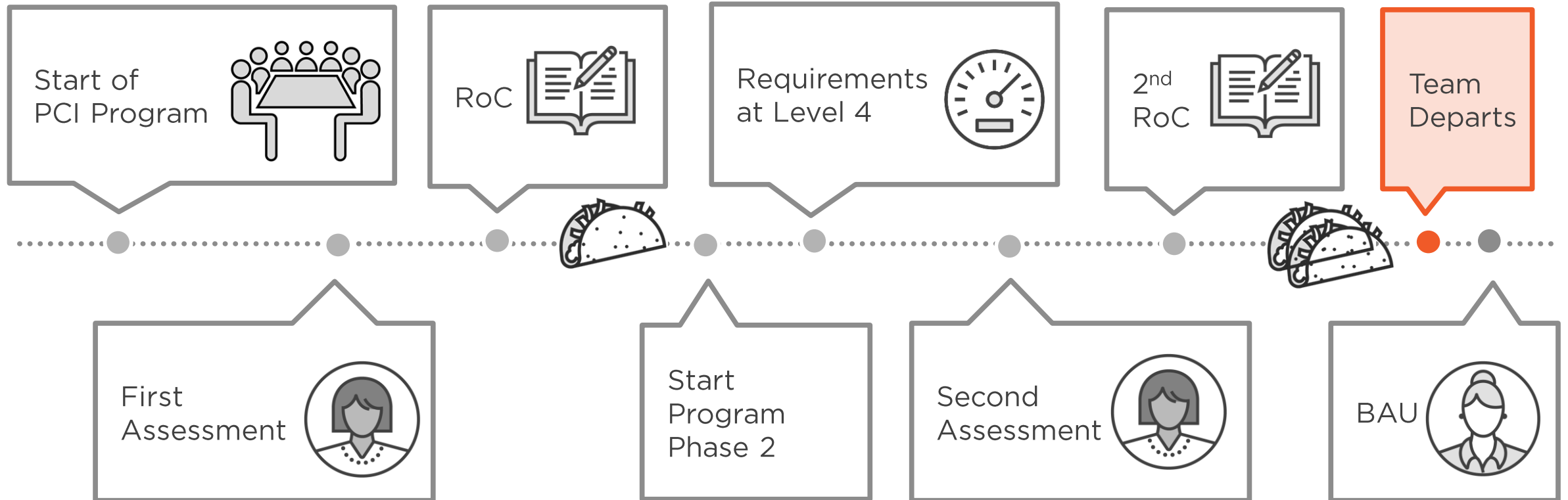
A Better Approach



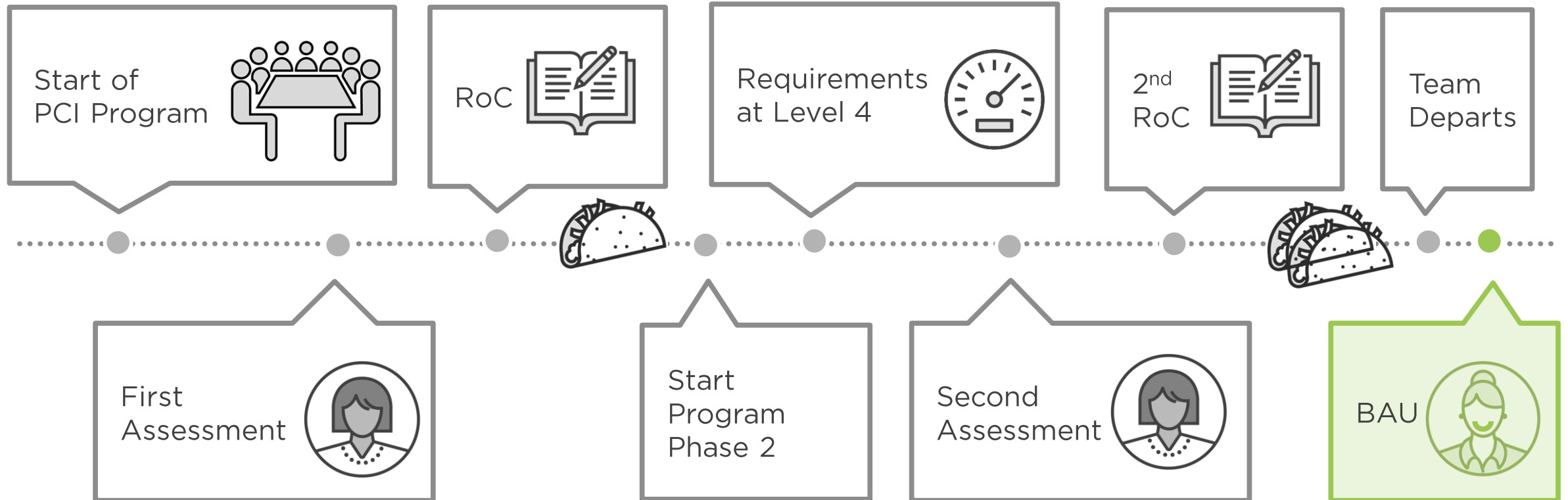
A Better Approach



A Better Approach



A Better Approach



PCI in Business Continuity



Systems pre-prepared for business continuity scenarios are not part of the cardholder data environment

- There's no cardholder data
- Build to be compliant

But in continuity situations they quickly become cardholder data environments

It's a significant change

- Gap assessment and remediation

It is fine to revisit scope
decisions after you have
become compliant



Jacob's View



Appendix A3: Designated Entities Supplemental Validation (DESV)

**“Things entities must do to
maintain PCI DSS compliance
between annual assessments”**



Who Is the DESV Intended For?



Whoever the Card Brands want it to be for

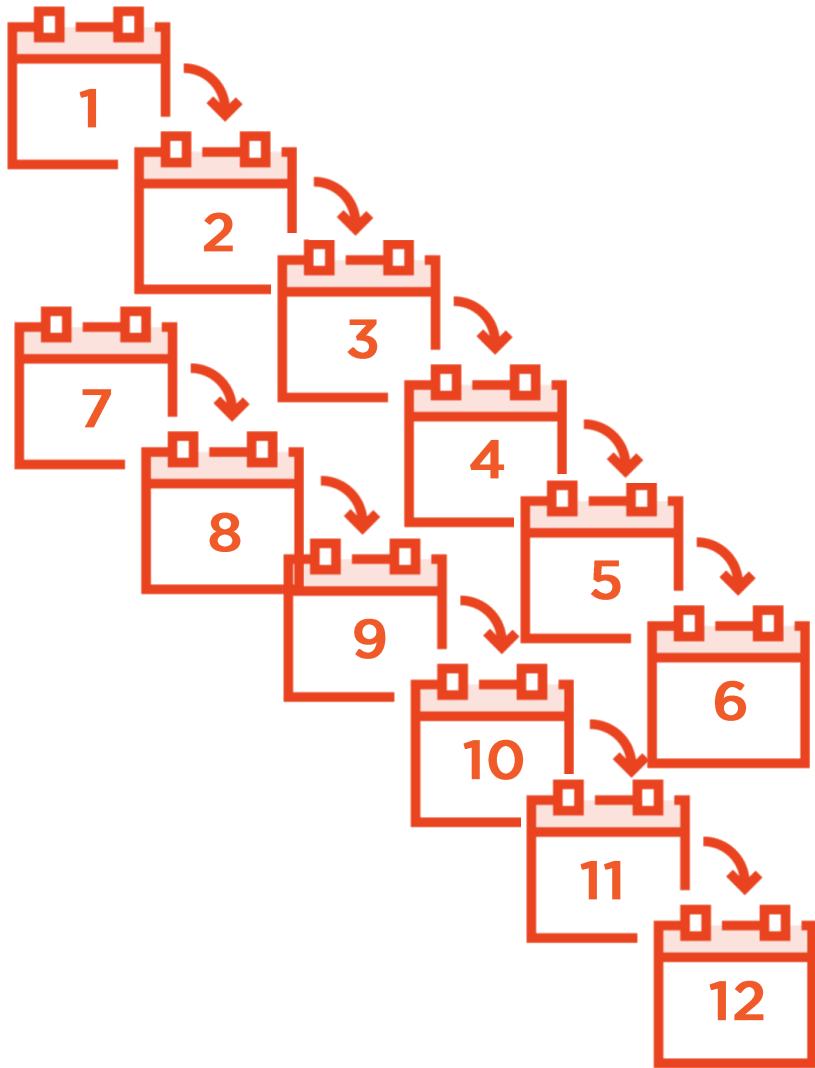
- Large volumes of cardholder data
- Aggregation points for cardholder data
- Compromised entities

Check Brand compliance programs



Anyone can use the DESV
to improve their
Business as Usual
PCI DSS Compliance





Requirements to ensure PCI DSS is embedded as Business as Usual (BAU)

Five requirements:

- Implement a PCI DSS compliance program
- Document and validate PCI DSS scope
- Validate PCI DSS is incorporated into business-as-usual (BAU) activities
- Control and manage logical access to the cardholder data environment
- Identify and respond to suspicious events



A3 Requirements	Testing Procedures	Guidance
A3.1 Implement a PCI DSS compliance program		
<p>A3.1.1 Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:</p> <ul style="list-style-type: none"> □ Overall accountability for maintaining PCI DSS compliance □ Defining a charter for a PCI DSS compliance program □ Providing updates to executive management and board of directors on PCI DSS compliance initiatives and issues, including remediation activities, at least annually <p>PCI DSS Reference: Requirement 12</p>	<p>A3.1.1.a Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance.</p> <p>A3.1.1.b Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized.</p> <p>A3.1.1.c Examine executive management and board of directors meeting minutes and/or presentations to ensure PCI DSS compliance initiatives and remediation activities are communicated at least annually.</p>	<p>Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities. Overall responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization.</p>
<p>A3.1.2 A formal PCI DSS compliance program must be in place to include:</p> <ul style="list-style-type: none"> □ Definition of activities for maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities □ Annual PCI DSS assessment processes □ Processes for the continuous validation of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement) □ A process for performing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions <p>PCI DSS Reference: Requirements 1-12</p>	<p>A3.1.2.a Examine information security policies and procedures to verify that processes are specifically defined for the following:</p> <ul style="list-style-type: none"> □ Maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities □ Annual PCI DSS assessment(s) □ Continuous validation of PCI DSS requirements □ Business-impact analysis to determine potential PCI DSS impacts for strategic business decisions 	<p>A formal compliance program allows an organization to monitor the health of its security controls, be proactive in the event that a control fails, and effectively communicate activities and compliance status throughout the organization.</p> <p>The PCI DSS compliance program can be a dedicated program or part of an over-arching compliance and/or governance program, and should include a well-defined methodology that demonstrates consistent and effective evaluation. Example methodologies include: Deming Circle of Plan-Do-Check-Act (PDCA), ISO 27001, COBIT, DMAIC, and Six Sigma.</p> <p style="text-align: right;"><i>(Continued on next page)</i></p>





Requirement A3.1

Implement a PCI DSS compliance program





Requirement A3.1.1

Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:



Requirement Detail

- **Overall accountability** for maintaining PCI DSS compliance
- Defining a **charter** for a PCI DSS compliance program
- Providing **updates to executive management** and **board of directors** on PCI DSS compliance initiatives and issues, including remediation activities, at least annually.





Requirement A3.1.2

A formal PCI DSS compliance program must be in place to include:



Requirement Detail

- Definition of activities for **maintaining and monitoring** overall PCI DSS compliance, including business-as-usual activities
- **Annual** PCI DSS **assessment** processes
- Processes for the **continuous validation** of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement)
- A process for performing **business-impact analysis** to determine potential PCI DSS impacts for strategic business decisions





Requirement A3.1.3

PCI DSS compliance **roles and responsibilities** must be specifically **defined** and formally **assigned** to one or more **personnel**, including at least the following:



Requirement Detail

- Managing PCI DSS **business-as-usual** activities
- Managing **annual** PCI DSS **assessments**
- Managing **continuous validation** of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement)
- Managing **business-impact analysis** to determine potential PCI DSS impacts for strategic business decisions





Requirement A3.1.4

Provide up-to-date PCI DSS and/or information security **training** at least annually to personnel with PCI DSS compliance responsibilities (as identified in A3.1.3)



Requirement Detail





Requirement A3.2

Document and validate PCI DSS scope





Requirement A3.2.1

Document and **confirm** the accuracy of **PCI DSS scope** at least **quarterly** and upon significant changes to the in-scope environment. At a minimum, the quarterly scoping validation should include:



Requirement Detail

- **Identifying** all **in-scope** networks and system components
- **Identifying** all **out-of-scope** networks and justification for networks being out of scope, including descriptions of all segmentation controls implemented
- **Identifying** all **connected entities**—e.g., third-party entities with access to the cardholder data environment (CDE)





Requirement A3.2.2

Determine PCI DSS scope **impact** for all **changes** to systems or networks, including additions of new systems and new network connections. Processes must include:



Requirement Detail

- Performing a formal PCI DSS impact assessment
- Identifying applicable PCI DSS requirements to the system or network
- Updating PCI DSS scope as appropriate
- Documented sign-off of the results of the impact assessment by responsible personnel (as defined in A3.1.3)





Requirement A3.2.2.1

Upon completion of a change, **all relevant PCI DSS requirements must be verified on all new or changed systems and networks**, and documentation must be updated as applicable.

Examples of PCI DSS requirements that should be verified include, but are not limited to:



Requirement Detail

- **Network diagram** is updated to reflect changes.
- Systems are configured per **configuration standards**, with all **default passwords changed** and unnecessary services disabled.
- Systems are protected with **required controls**—e.g., **file-integrity monitoring (FIM)**, **anti-virus**, **patches**, **audit logging**.
- Verify that **sensitive authentication data (SAD)** is **not stored** and that all cardholder data (CHD) storage is documented and incorporated into data- retention policy and procedures
- New systems are included in the **quarterly vulnerability scanning** process.





Requirement A3.2.3

Changes to **organizational structure**— for example, a company merger or acquisition, change or reassignment of personnel with responsibility for security controls—result in a **formal** (internal) **review** of the **impact** to **PCI DSS scope** and applicability of controls.



Requirement Detail





Requirement A3.2.4

If **segmentation** is used, confirm PCI DSS scope by performing **penetration testing** on **segmentation controls** at least **every six months** and after any changes to segmentation controls/methods.



Requirement Detail





Requirement A3.2.5

Implement **a data-discovery** methodology to confirm PCI DSS scope and to **locate** all **sources** and **locations** of **clear-text PAN** at least **quarterly** and upon significant changes to the cardholder environment or processes.



Requirement Detail

Data-discovery methodology must take into consideration the potential for clear-text PAN to reside on systems and networks outside of the currently defined CDE.





Requirement A3.2.5.1

Ensure effectiveness of methods used for **data discovery**—e.g., methods must be able to discover clear-text PAN on all types of system components (for example, on each operating system or platform) and file formats in use.



Requirement Detail

The effectiveness of data-discovery methods must be confirmed at least annually.





Requirement A3.2.5.2

Implement response procedures to be initiated upon the **detection** of clear-text **PAN outside** of the **CDE** to include:



Requirement Detail

- Procedures for determining **what to do** if clear-text PAN is discovered outside of the CDE, including its retrieval, secure deletion and/or migration into the currently defined CDE, as applicable
- Procedures for determining **how the data ended up outside of the CDE**
- Procedures for **remediating** data **leaks** or process **gaps** that resulted in the data being outside of the CDE
- Procedures for **identifying** the **source** of the **data**
- Procedures for identifying whether any track data is stored with the PANs





Requirement A3.2.6

Implement mechanisms for **detecting** and **preventing** clear-text **PAN** from **leaving** the **CDE** via an unauthorized channel, method, or process, including generation of audit logs and alerts.



Requirement Detail





Requirement A3.2.6.1

Implement **response procedures** to be initiated upon the **detection** of attempts to remove **clear-text PAN** from the **CDE** via an unauthorized channel, method, or process.

Response procedures must include:



Requirement Detail

- Procedures for the **timely investigation** of alerts by responsible personnel
- Procedures for **remediating** data **leaks** or process **gaps**, as necessary, to prevent any data loss





Requirement A3.3

Validate PCI DSS is incorporated into business-as-usual (BAU) activities





Requirement A3.3.1

Implement a process to **immediately detect** and **alert** on **critical security control failures**.

Examples of critical security controls include, but are not limited to:



Requirement Detail

- Firewalls
- IDS/IPS
- FIM
- Anti-virus
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation controls (if used)





Requirement A3.3.1.1

Respond to failures of any **critical** security **controls** in a **timely** manner.

Processes for responding to failures in security controls must include:



Requirement Detail

- **Restoring** security functions
- Identifying and documenting the duration (date and time start to end) of the security failure
- **Identifying** and **documenting cause**(s) of failure, including root cause, and documenting remediation required to address root cause
- Identifying and addressing any security issues that arose during the failure
- Performing a risk assessment to determine whether further actions are required as a result of the security failure
- **Implementing controls** to **prevent** cause of failure from **reoccurring**
- Resuming monitoring of security controls





Requirement A3.3.2

Review hardware and **software** technologies at least **annually** to confirm whether they continue to **meet** the organization's **PCI DSS requirements**.

(For example, a review of technologies that are no longer supported by the vendor and/or no longer meet the security needs of the organization.)



Requirement Detail

The process includes a plan for remediating technologies that no longer meet the organization's PCI DSS requirements, up to and including replacement of the technology, as appropriate.





Requirement A3.3.3

Perform **reviews** at least **quarterly** to **verify BAU activities** are being followed.

Reviews must be performed by personnel assigned to the PCI DSS compliance program (as identified in A3.1.3), and include the following:



Requirement Detail

- Confirmation that all BAU activities (e.g., A3.2.2, A3.2.6, and A3.3.1) are being performed
- Confirmation that personnel are following security policies and operational procedures (for example, daily log reviews, firewall rule-set reviews, configuration standards for new systems, etc.)
- Documenting how the reviews were completed, including how all BAU activities were verified as being in place.
- Collection of documented evidence as required for the annual PCI DSS assessment
- Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program (as identified in A3.1.3)
- Retention of records and documentation for at least 12 months, covering all BAU activities



Requirement A3.4

Control and manage logical access to the cardholder data environment





Requirement A3.4.1

Review user accounts and access privileges to in-scope system components at least **every six months** to ensure user accounts and access remain appropriate based on job function, and authorized.



Requirement Detail





Requirement A3.5

Identify and respond to suspicious events





Requirement A3.5.1

Implement a methodology for the **timely identification** of **attack patterns** and **undesirable behavior** across systems—for example, using coordinated manual reviews and/or **centrally managed or automated log- correlation tools**—to include at least the following:



Requirement Detail

- Identification of anomalies or suspicious activity as it occurs
- Issuance of timely alerts upon detection of suspicious activity or anomaly to responsible personnel
- Response to alerts in accordance with documented response procedures

Designated
Entity
Supplemental
Validation
(DESV)

Requires a dedicated assurance function

Controls at maturity level 4

Significant investment

Not a compulsory part of the standard

- Card Bands may require it

Anyone can use it voluntarily



Be Secure Be Compliant



Security is more important than compliance

Understand who is asking you be comply with PCI DSS, and why

Before you start, understand the destination

Design your systems to do as little PCI DSS as you possibly can

Include a year's transition to BAU after your first assessment as part of any PCI compliance project / program

Actively control change



PCI DSS: The State of Cardholder Data Attacks

by Aaron Willis and John Elliott

In this course, you'll learn about the criminals' ways of working from an experienced (PFI) Forensic Investigator and discover what actually happens in the course of a PCI forensic investigation.

[Start Course](#)[Bookmark](#)[Add to Channel](#)[Download Course](#)[Table of contents](#)[Description](#)[Transcript](#)[Exercise files](#)[Discussion](#)[Related Courses](#)

This course is part of:  Payment Card Industry Data Security Standard (PCI DSS) Path

[Expand All](#)[Course Overview](#)

1m 47s

[Understanding the Forensic Collection Process](#)

27m 42s

[Understanding the Threat Landscape - Point of Sale \(POS\) Attacks](#)

18m 44s

[Understanding the Threat Landscape - eCommerce Attacks](#)

18m 50s

[Understanding the Threat Landscape - Infrastructure Attacks](#)

18m 54s

