

A large, stylized globe in shades of blue and cyan dominates the background. It is overlaid with a network of glowing white lines and dots, representing global connectivity and data flow. The globe is shown from a perspective that includes North and South America.

From theory to practice DNSSEC for postal operators

June 2026

Why postal operators should care

Why?

Postal operators run some of the most public-facing digital services in a country: tracking, notifications, ecommerce, exchange, customer identity, and official
Attackers exploit that trust through domain phishing and spoofing.

When DNS fails customers lose confidence fast: fake fake tracking links, diverted portals, fraudulent mail mail domains.

DNSSEC is relevant because the domain name part of the trust model.

Trust

National brand, citizen-facing services, communications.

Risk

Phishing, spoofing and redirection domain layer first.

Impact

Fraud, outage, reputational damage and and broken partner integrations.

Where DNSSEC fits in the control stack

What DNSSEC
gives you

**Integrity and
authenticity**

Resolvers can validate that DNS
data came from the right
right zone and was not modified
modified in transit.

What DNSSEC
does not do

Encryption

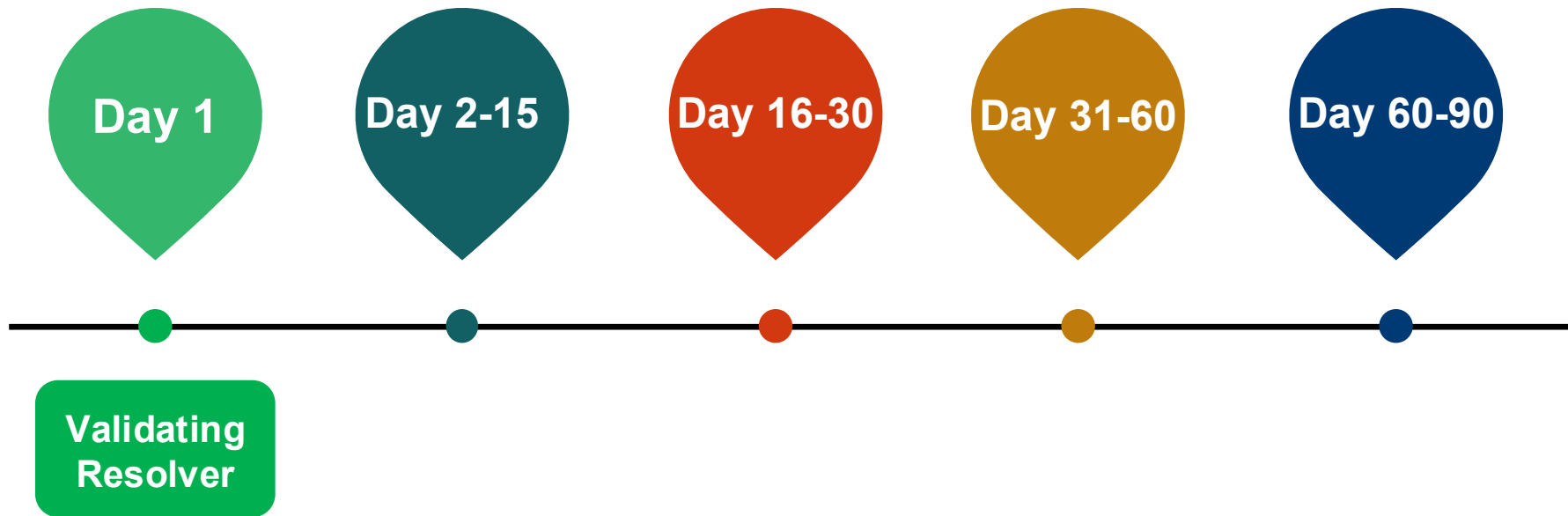
It does not replace TLS, mail
authentication, endpoint security,
security, registry controls or
incident response.

Operational
lesson

**Runbook
not checkbox**

The real challenge is keeping the
the chain of trust intact through
through the full delivery chain.
chain.

The plan



Validating g Resolver Resolver

This is a low risk action.

It immediately protects your internal users systems from spoofing.

It allows your operators to gain first with DNSSEC.

Trust

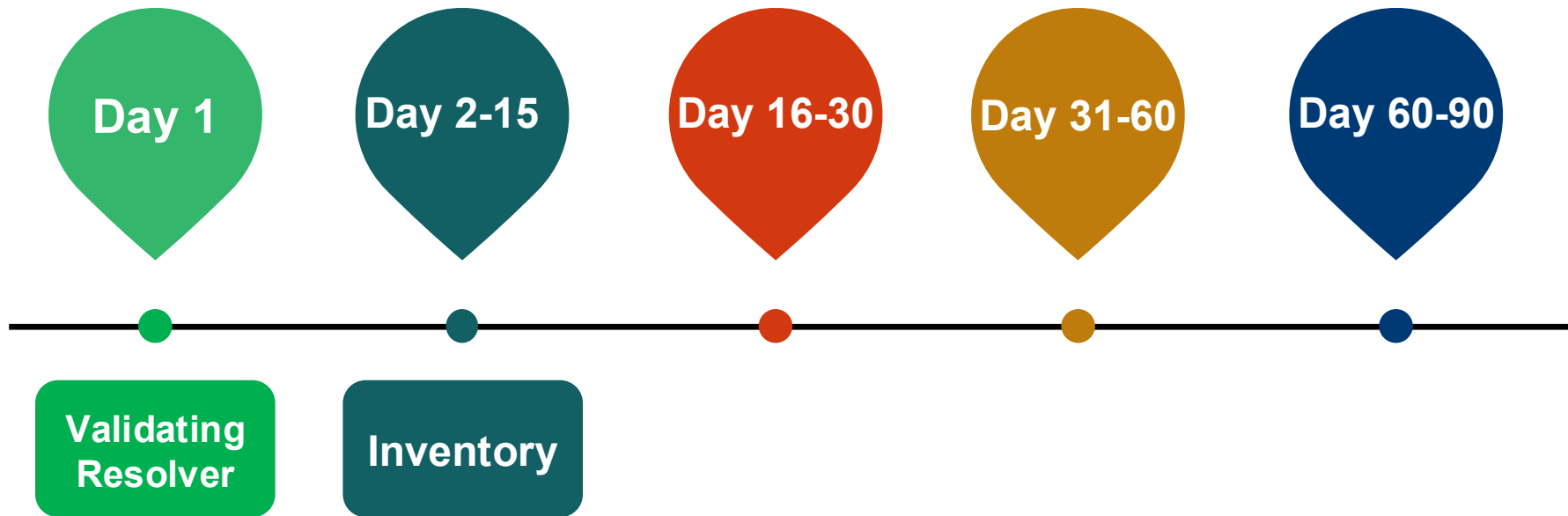
You can start trusting the existing infrastructure.

Low Risk

No impact on your domain names.

Impact

Your own networks are now protected against spoofing.



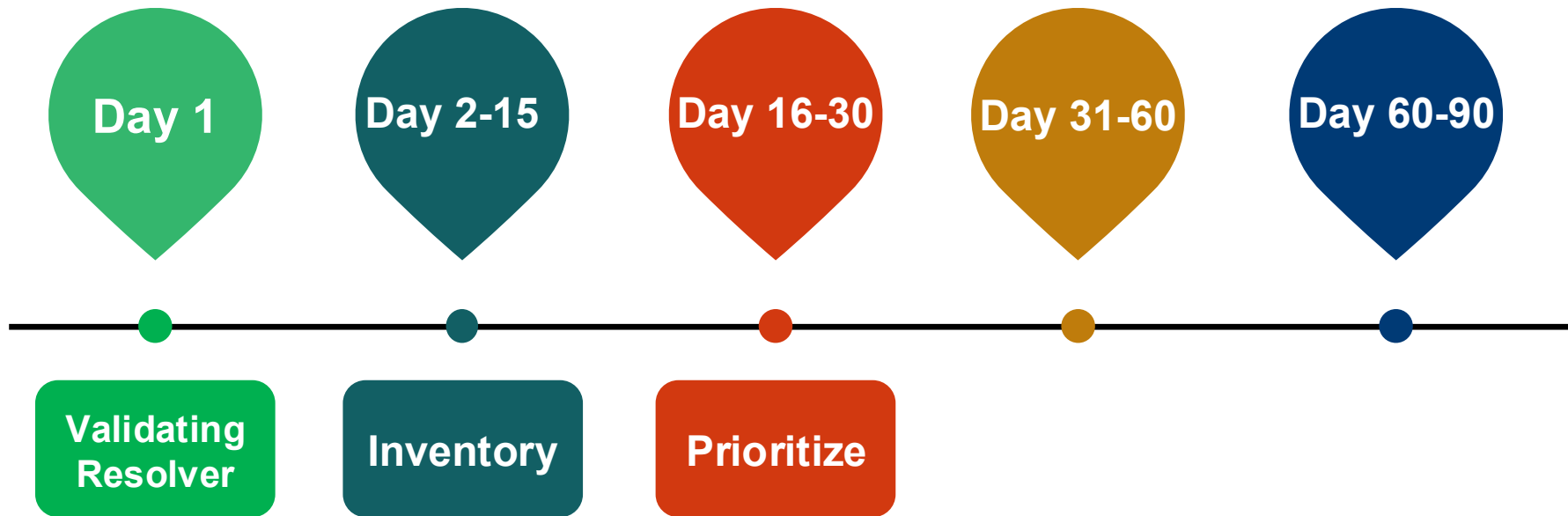
Inventory

Document ownership

- List all domains, subdomains, providers and registrars.
- Not just your own domains, also from service providers, partners, SaaS
- Which domains are your name using?

Impact

You get an overview over the work ahead of ahead of you and you can start to prioritize prioritize work.



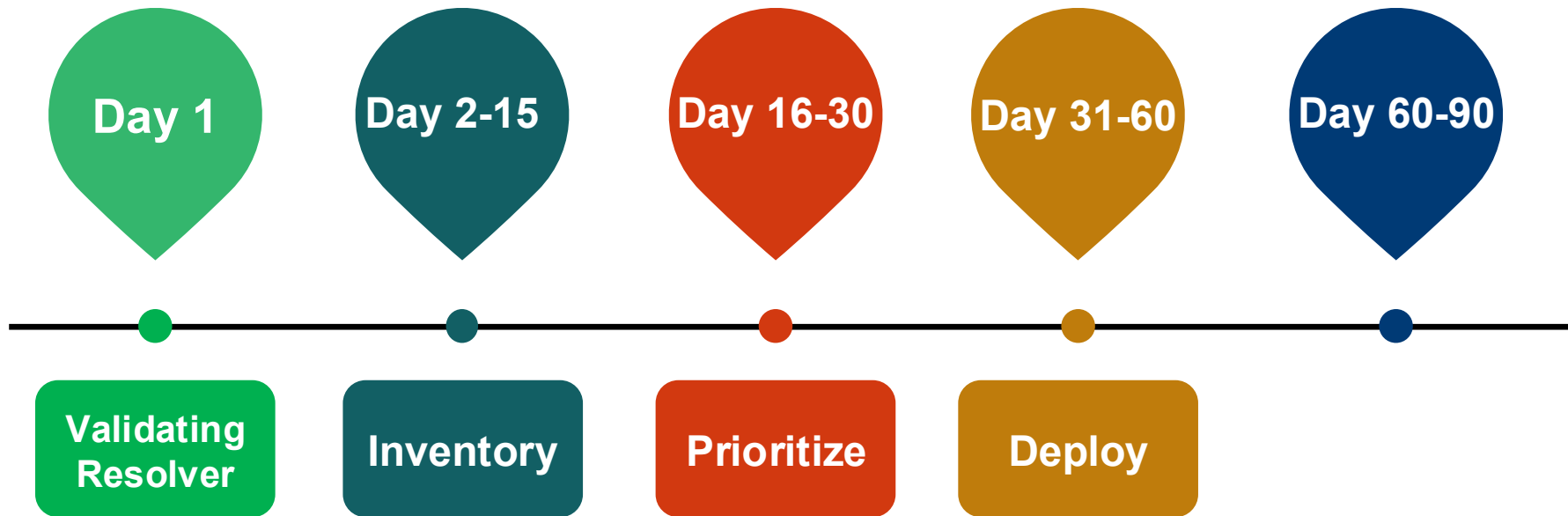
Prioritize

High priority zones

- Public website and ecommerce storefront
- Tracking and customer notification domains
- Customer login, SSO and app backends
- APIs for merchants, customs and partners
- Mail-related domains and outbound link domains

Impact

Now you know they way ahead.



Deploy

Sign the first zones

- Decide on DNSSEC parameters
- Do one domain after the other
- No changes on Fridays

Trust

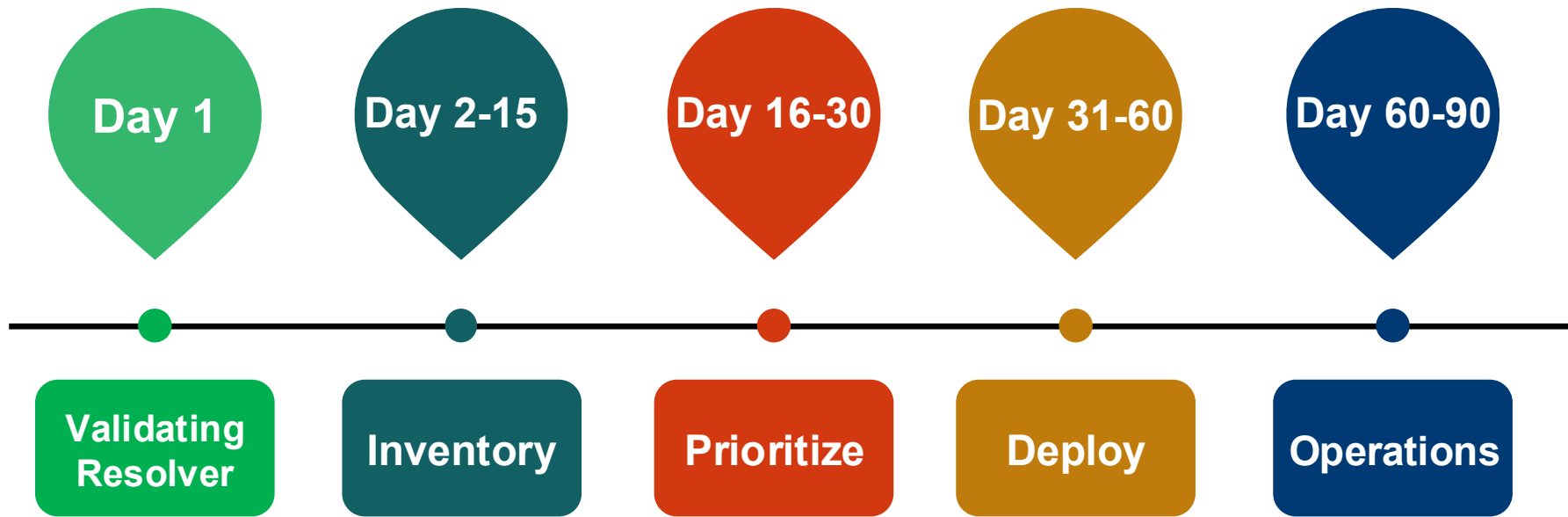
Customers can start trusting your

Risk

Brand reputation risks outweighs operational operational risk.

Impact

Customers are protected from phishing.



Operations

Checks & Balances

- Protect private keys
- Plan rollovers
- Monitor signatures
- Drill incidents

Trust

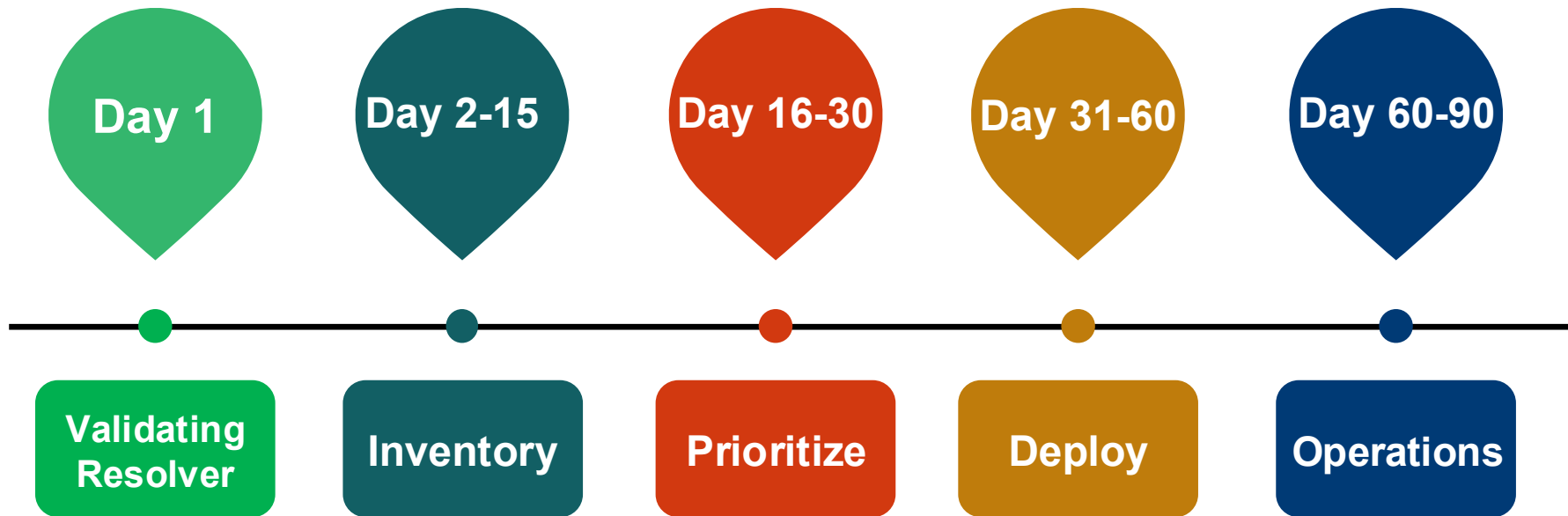
Your internal IT has control over the

Risk

These practices lower your operational risk risk significantly.

Impact

Domains and with that business stay online.
online.



DNSSEC should be treated as part of a postal operator's trust architecture — protecting the names customers, merchants, governments and partners rely on every day.

-  icann.org
-  [@icann](https://twitter.com/icann)
-  facebook.com/icannorg
-  youtube.com/icannnews
-  flickr.com/icann
-  linkedin.com/company/icann
-  instagram.com/icannorg