M3AAWG
MESSAGING MALWARE MOBILE

M3AAWG DMARC Training Series

Mike Adkins, Paul Midgen
DMARC.org
October 22, 2012

M³AAWG DMARC Training Videos

(2.5 hours of training)

This is Segment 6 of 6

The complete series of DMARC training videos is available at:
https://www.m3aawg.org/activities/maawg-training-series-videos

Segment 1 **What is DMARC?** **(about 20 minutes)**	**Segment 2** **DMARC Identifier Alignment** **(about 20 minutes)**	**Segment 3** **DMARC Policy Records** **(about 30 minutes)**
Segment 4 **DMARC Reporting** **(about 15 minutes)**	**Segment 5** **DMARC Information for Mailbox Providers** **(about 20 minutes)**	**Segment 6** **DMARC Information for Domain Owners and 3rd Parties** **(about 40 minutes)**

M3AAWG
MESSAGING MALWARE MOBILE

DMARC Information for Doman Owners and 3rd Parties

DMARC Segment 6 – about 40 minutes

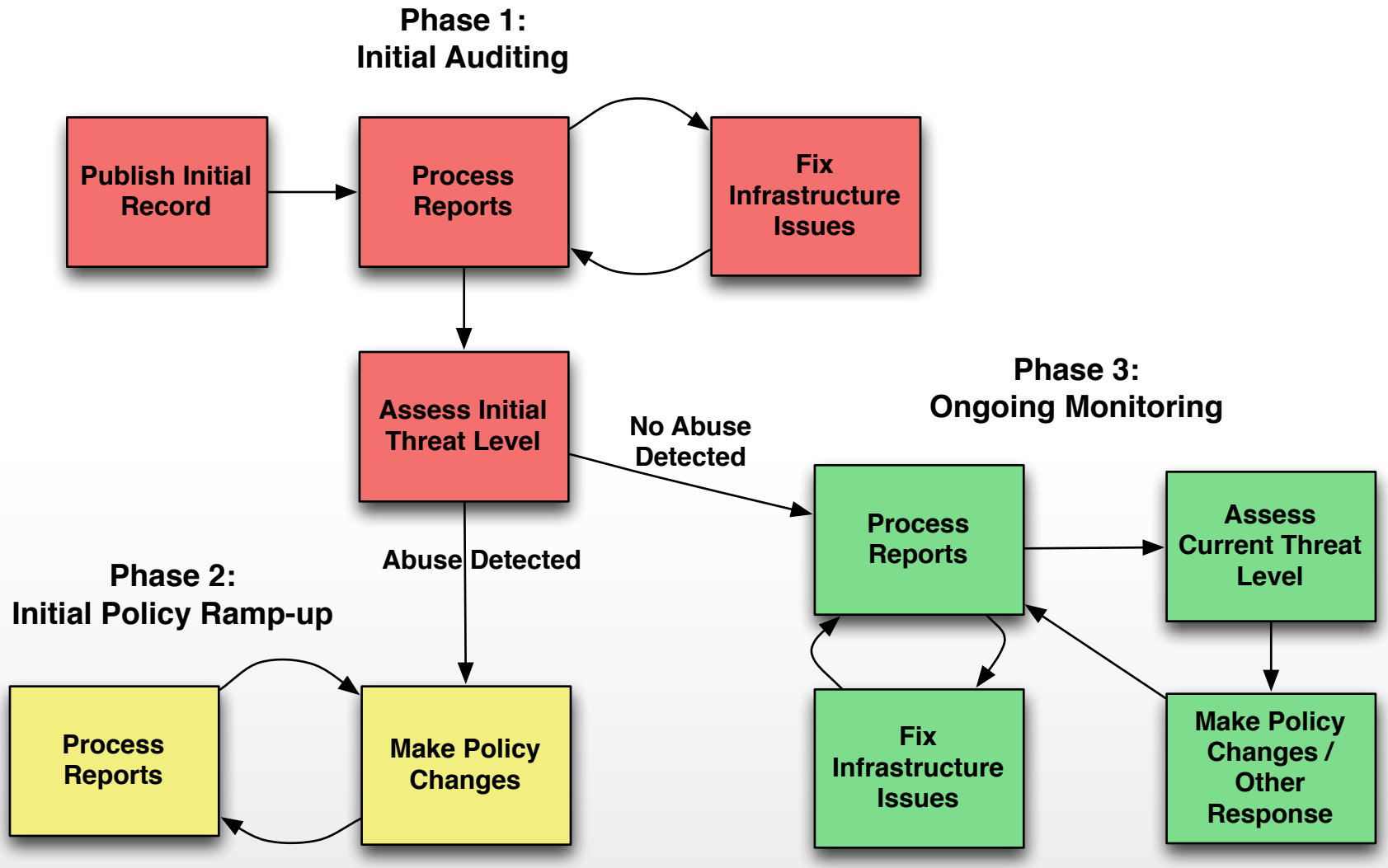
Michael Adkins, DMARC.org and M3AAWG Co-Vice Chairman

October 22, 2012

Information for Domain Owners

- The Reporting and Compliance Process
  - Initial Record Publishing
  - 3rd Party Deployment Profiles
  - Report Processing and Analysis
  - Rolling out Policies
  - Long Term Monitoring

The Reporting and Compliance Process For Domain Owners



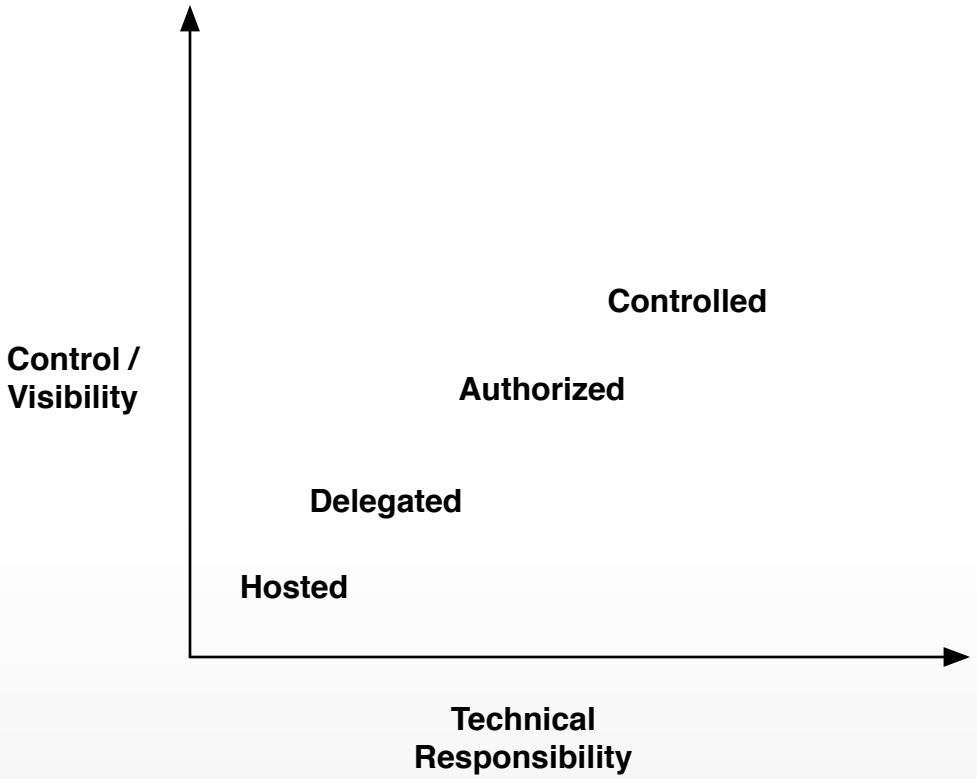
Initial Record Publishing

M3AAWG
MESSAGING MALWARE MOBILE

Everyone's first DMARC record

```
v=DMARC1; p=none; rua=mailto:aggregate@example.com;
```

3rd Party Deployment Profiles



Controlled – The Domain Owner fully controls their own DNS, and wants as much control over their email as possible.

Authorized – The Domain Owner lets the 3rd party dictate the content of some DNS records, while still retaining some operational control.

Delegated – The Domain Owner delegates control of their DNS to the 3rd party, and wants to be mostly hands-off with their email.

Hosted – The Domain Owner allows the 3rd party to handle everything, and has little control

3rd Party Deployment Profiles

Controlled

The Domain Owner retains control of the domain or subdomain, provides a DKIM signing key to 3rd party and publishes the public key, and includes the appropriate information in their SPF record.

Pro

- This scenario allows 3rd parties to send as the organizational domain if desired.
- The Domain Owner retains operational control.

Cons

- Coordination between the domain owner and the 3rd party mailer is required to ensure proper DKIM key rotation, accurate SPF records, etc.
- Risk of coordination overhead/issues increases as the number of bilateral relationships increase for domain owners and vendors.

3rd Party Deployment Profiles

Controlled

Contractual points

- Process for DKIM key rotation. Obligations of each party, including testing.

- SPF record requirements and process for adding new hosts.

3rd Party Deployment Profiles

Authorized

Similar to Controlled Profile, except the 3rd party creates the DKIM key pair and generally takes a more active role in dictating record content. This approach is useful for Domain Owners where a different 3rd party is providing DNS and other services for the domain.

Pros

- Can streamline provisioning for the 3rd party.
- One less task for the Domain Owner.

Cons

- Can create additional management issues for Domain Owners who use multiple 3rd parties.
- Possible additional contractual point for key strength requirements.

3rd Party Deployment Profiles

Delegated

The Domain Owner delegates a subdomain to 3rd party mailer and relies on contractual relationship to ensure appropriate SPF records, DKIM signing, and DMARC records.

Pros

- Reduces Domain Owner implementation issues to mostly contractual.
- The 3rd party is responsible for SPF records, DKIM signing and publishing, etc.
- Domain owner may still be responsible for ensuring Identifier Alignment.

Con

- The Domain Owner potentially gives up day to day control and visibility into operations and conformance.

3rd Party Deployment Profiles

Delegated

Contractual points

- Creation and maintenance of SPF, DKIM and DMARC records
- (Quarterly) Rotation of DKIM keys and minimum length of key (1024 recommended)
- Investigation of DMARC rejections
- Handling of DMARC Reports
- Requirements for reporting back to the Domain Owner
- Indemnification (if any) for mail lost due to improper records or signatures.

3rd Party Deployment Profiles

Hosted

The 3rd party is also providing DNS, webhosting, etc for the Domain Owner and makes the process mostly transparent to the domain owner.

Pro

- Very easy for less sophisticated Domain Owners.
- Can be mostly automated by the 3rd party.

Con

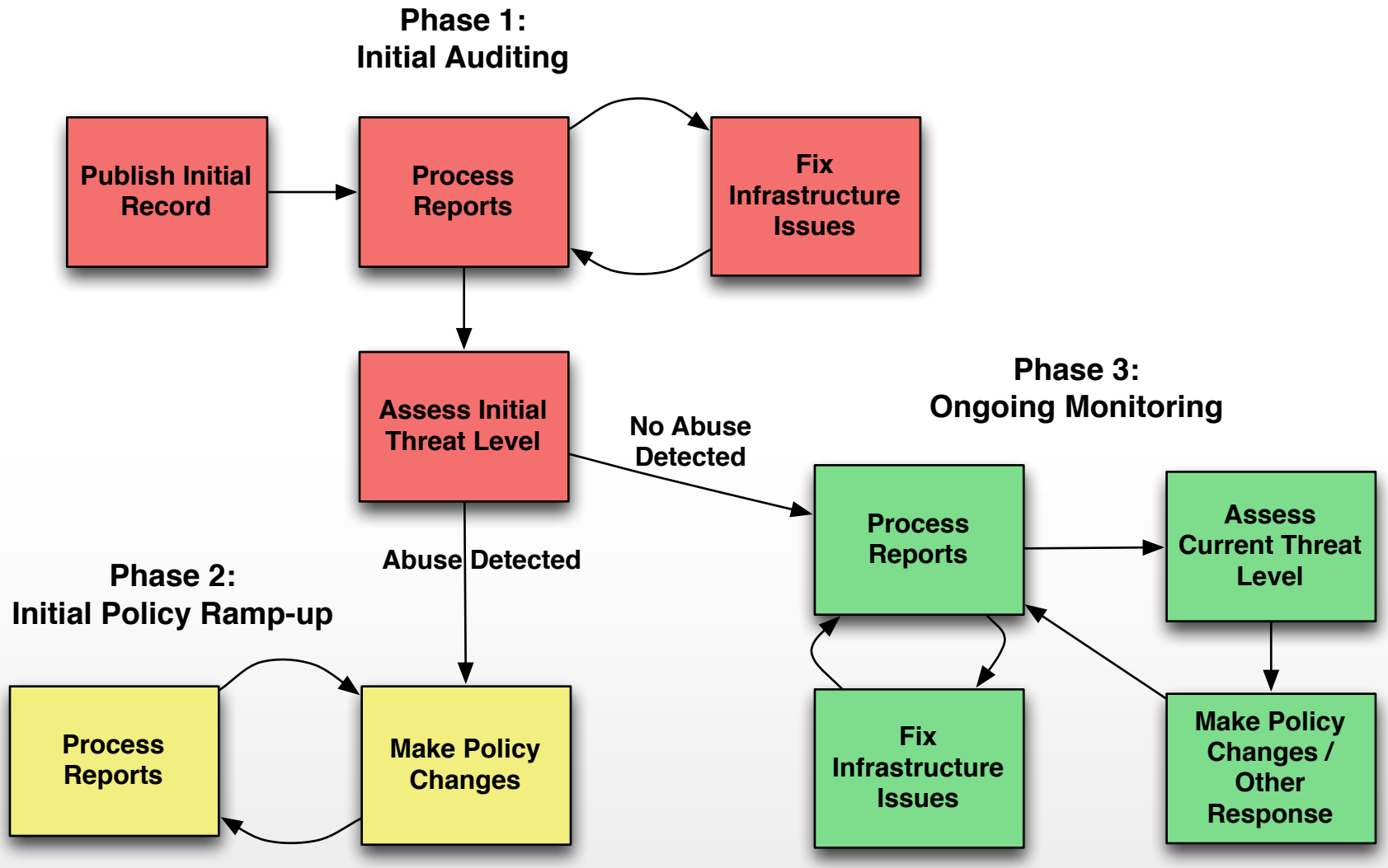
- The domain owner is significantly more dependent on the 3rd party.

3rd Party Deployment Profiles

3rd Party responsibilities

	Controlled	Authorized	Delegated	Hosted
Provide SPF record content	Y	Y	Y	Y
Maintain SPF records	N	N	Y	Y
Maintain DKIM records	N	N	Y	Y
Create DKIM Keys	N	Y	Y	Y
Rotate DKIM Keys	Y	Y	Y	Y
Maintain DMARC Records	N	N	Y	Y
Process DMARC reports	N	?	?	Y

Report Processing and Analysis



Report Processing and Analysis

Report Parsing Tools

http://dmarc.org/resources.html

If you develop report parsing tools you are willing to share, please send a note to the dmarc-discuss list and let us know.

Report Processing and Analysis

M3AAWG
MESSAGING MALWARE MOBILE

Step 1: Categorize the IPs in the Aggregate Report

- Your Infrastructure
- Authorized 3rd Parties
- Unauthorized 3rd Parties *

* - You should consider everything an Unauthorized 3rd Party by default.

Report Processing and Analysis – Infrastructure Auditing

Step 2: Infrastructure Auditing

For both your Infrastructure and Authorized 3rd Parties

- Identify owners
- LOE for Deploying Domain Authentication
- LOE for Identifier Alignment
- Business case / Justification

Report Processing and Analysis

M3AAWG
MESSAGING MALWARE MOBILE

Step 3: Identify Malicious Email

Research Unauthorized 3rd Parties and label the Abusers

- Use public data sources
- Vendor services
- Look for known failure cases
- Forensic reports

Report Processing and Analysis

Step 4: Perform Threat Assessment

Categories

- Your Infrastructure
- Authorized 3rd parties
- Unauthorized 3rd parties
- Abusers

Calculate the Sum of Unaligned Email from each Category

Report Processing and Analysis

Step 4: Perform Threat Assessment

Phish = Unaligned Email From Abusers

Definite False Positives = Unaligned Email from Your Infrastructure + Unaligned Email from Authorized 3rd parties

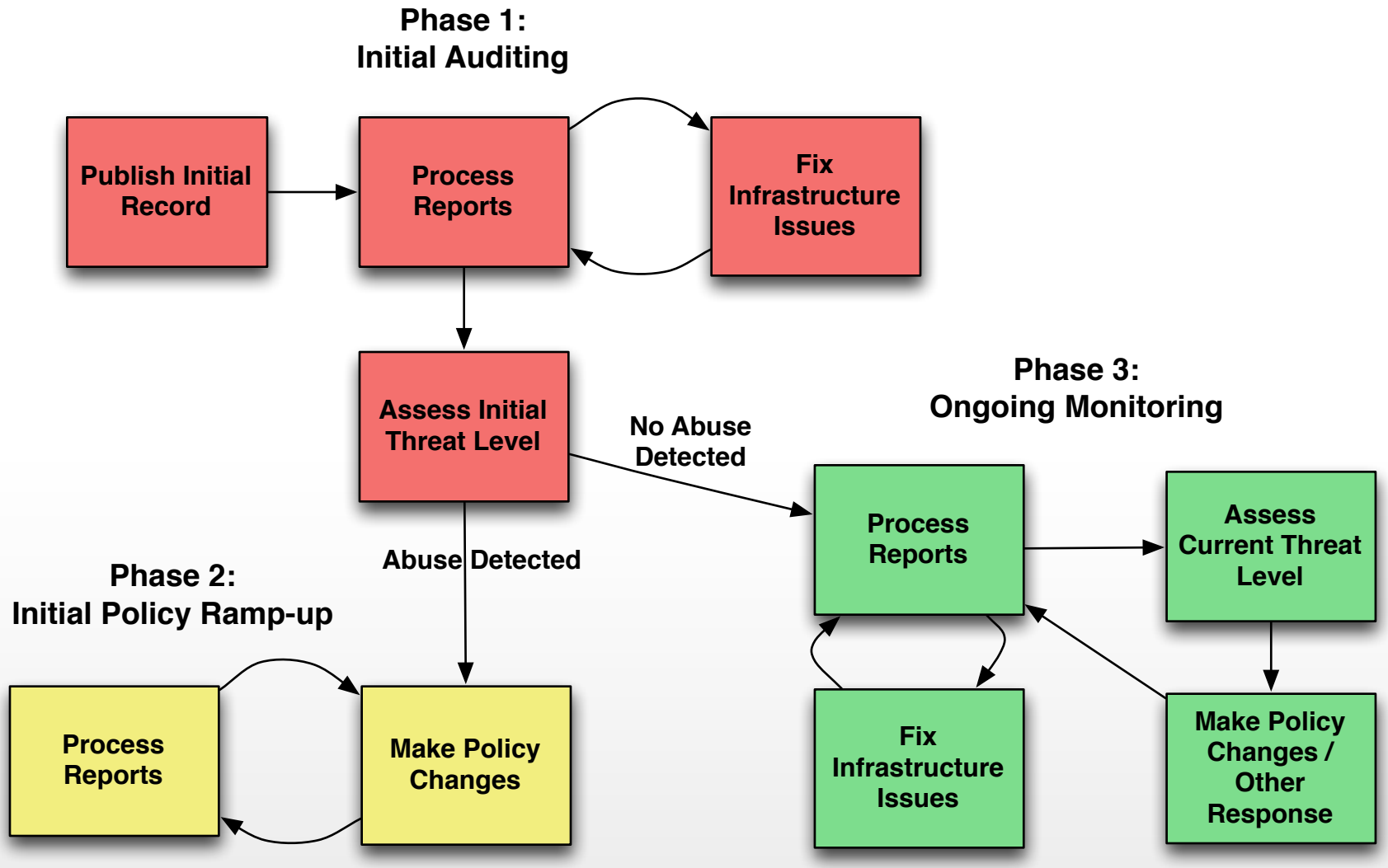
Potential False Positives = Unaligned Email from Unauthorized 3rd parties

Consider:

- Phish vs. False Positives
- Phish vs. Total Aligned Email

If there is no Phish, you don't have a Domain Spoofing problem and don't need to move forward with DMARC policies.

Initial Policy Ramp-up



Initial Policy Ramp-up

Step 1: Verify Authentication and Alignment for all of your Infrastructure and all Authorized 3rd Parties.

Step 2: Update your record to:

```
p=quarantine; pct=10;
```

Do not:

- Skip ‘quarantine’ and go straight to ‘reject’
- Change the policy action from ‘none’ without setting a ‘pct’

Initial Policy Ramp-up

Step 3: Monitor your reports for issues and address them.

Make a ‘go forward / go back’ decision.

Step 4: Update your record to increase the ‘pct’.

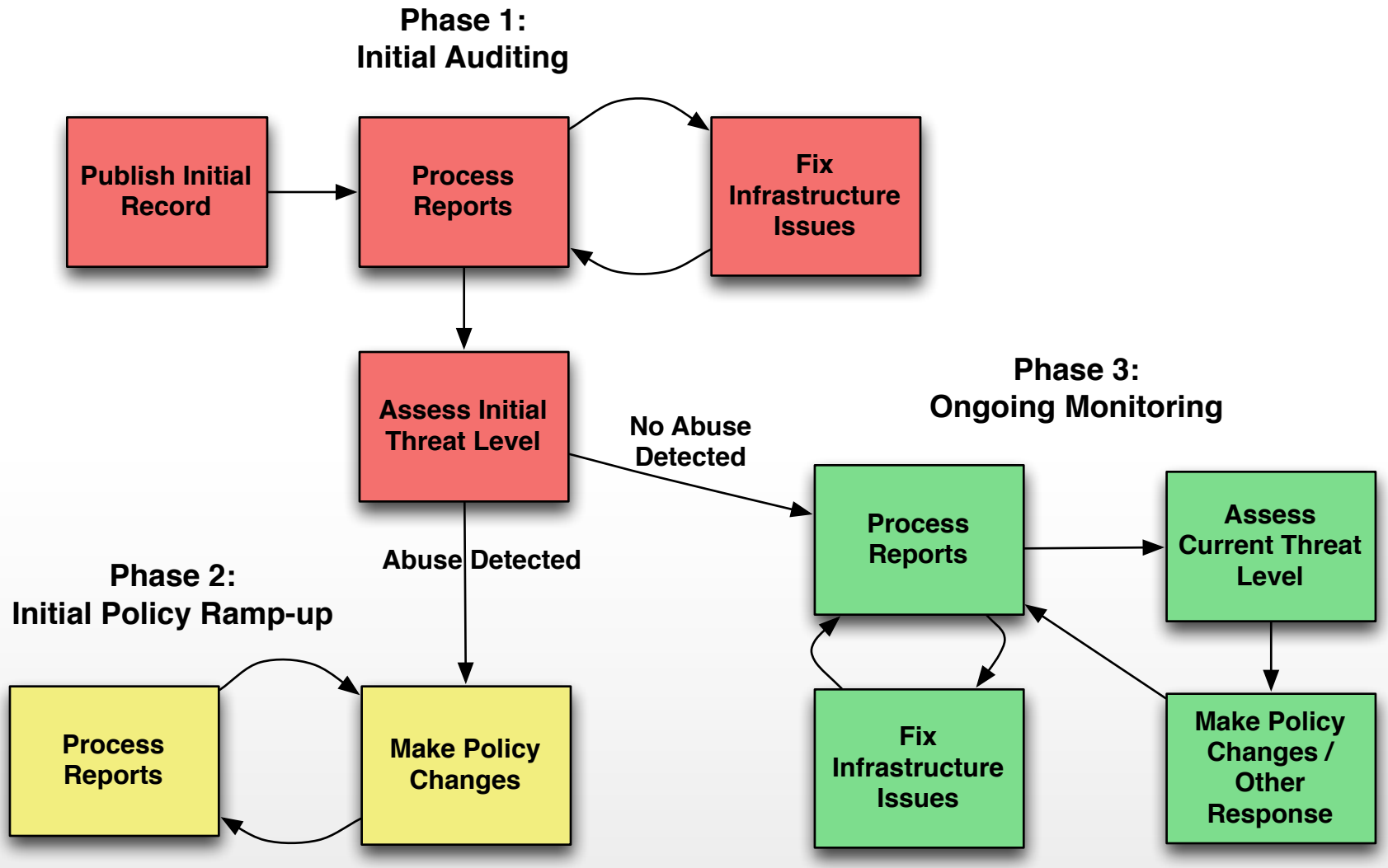
Rinse and repeat until you get to ‘pct=100’.

Initial Policy Ramp-up

Step 5: If needed, update your record to:

```
p=reject
```

Ongoing Monitoring



Ongoing Monitoring

- Categorize new IPs in Aggregate reports
  - Your Infrastructure
  - Authorized 3rd Parties
  - Unauthorized 3rd Parties
  - Abusers

- Reassess the Threat Level
  - Increases in phish
  - Changes in unaligned email volume
  - Make changes accordingly
  - Takedowns or other phish responses

Ongoing Monitoring

Be on the look out for:

- Infrastructure changes
- New products / new subdomains
- New authorized 3rd parties
- Mergers and acquisitions

Resources

M3AAWG
MESSAGING MALWARE MOBILE

Dmarc.org

Resources page for tools
Participate page for list sign up

This has been the sixth of six DMARC video segments

View the entire

M³AAWG DMARC Training Series

from the public training video pages on the M³AAWG website at:
https://www.m3aawg.org/activities/maawg-training-series-videos

Our thanks to Michael Adkins, Paul Midgen and DMARC.org
for developing the material in this series and allowing M³AAWG to videotape it
for professionals worldwide. Thanks to Message Bus for additional videotaping
and to videographer Ilana Rothman.

This video is presented by the
Messaging, Malware and Mobile Anti-Abuse Working Group

For information about M3AAWG:
www.m3aawg.org
www.facebook.com/maawg
www.twitter.com/maawg
www.youtube.com/maawg

Contact us at:
https://www.m3aawg.org/contact_form