



A Maturity Model for Enterprise Key Management

Lessons Learned

Agenda



- ▶ Problem statement
- ▶ Approach
 - ▶ Framework
 - ▶ Maturity model
- ▶ Applying the model
- ▶ Gaps and lessons learned
- ▶ Conclusions

Problem statement

Companies have struggled with

How to manage encryption keys

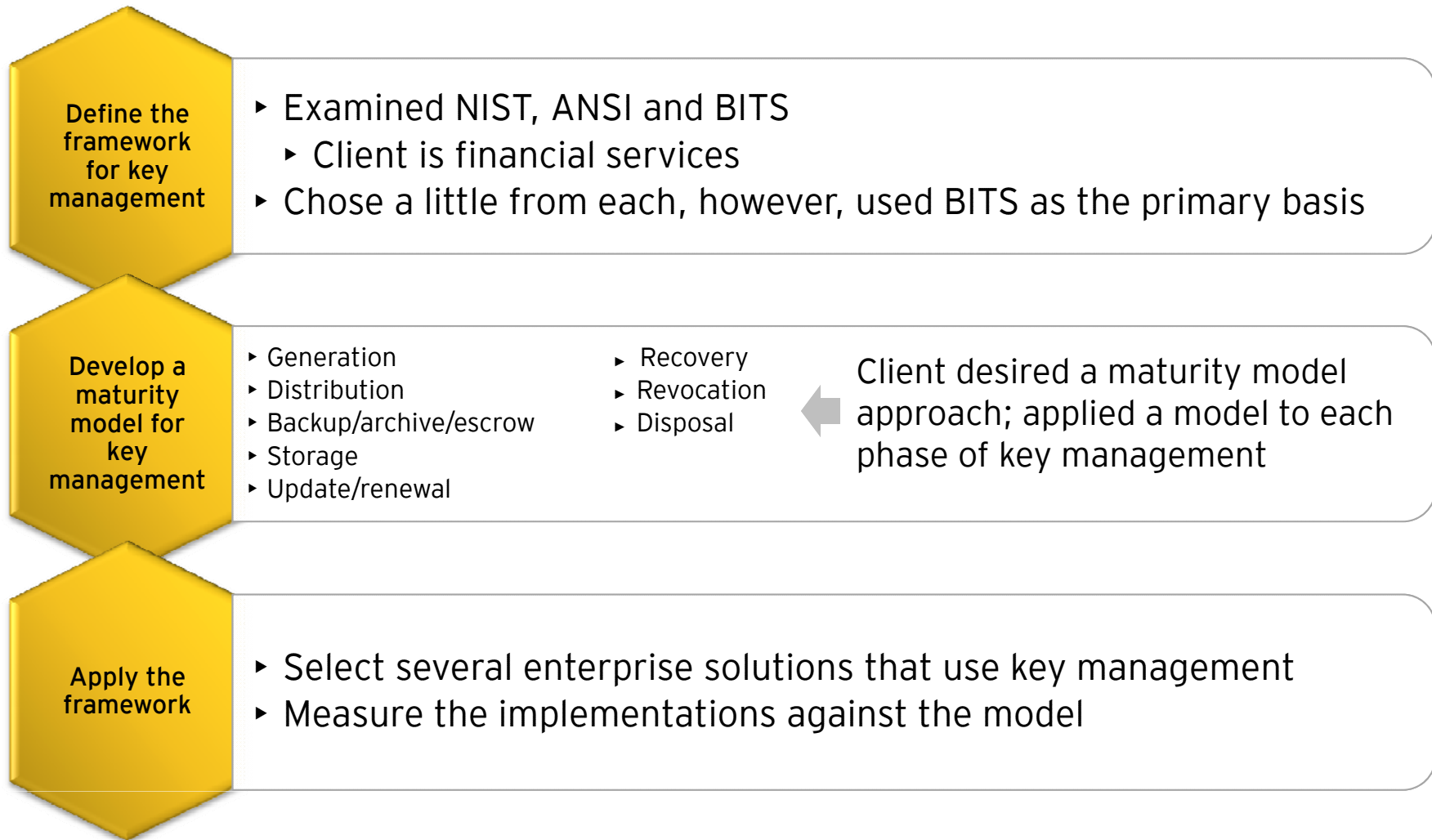
Provide consistent guidance to key custodians

Measure successful key management programs

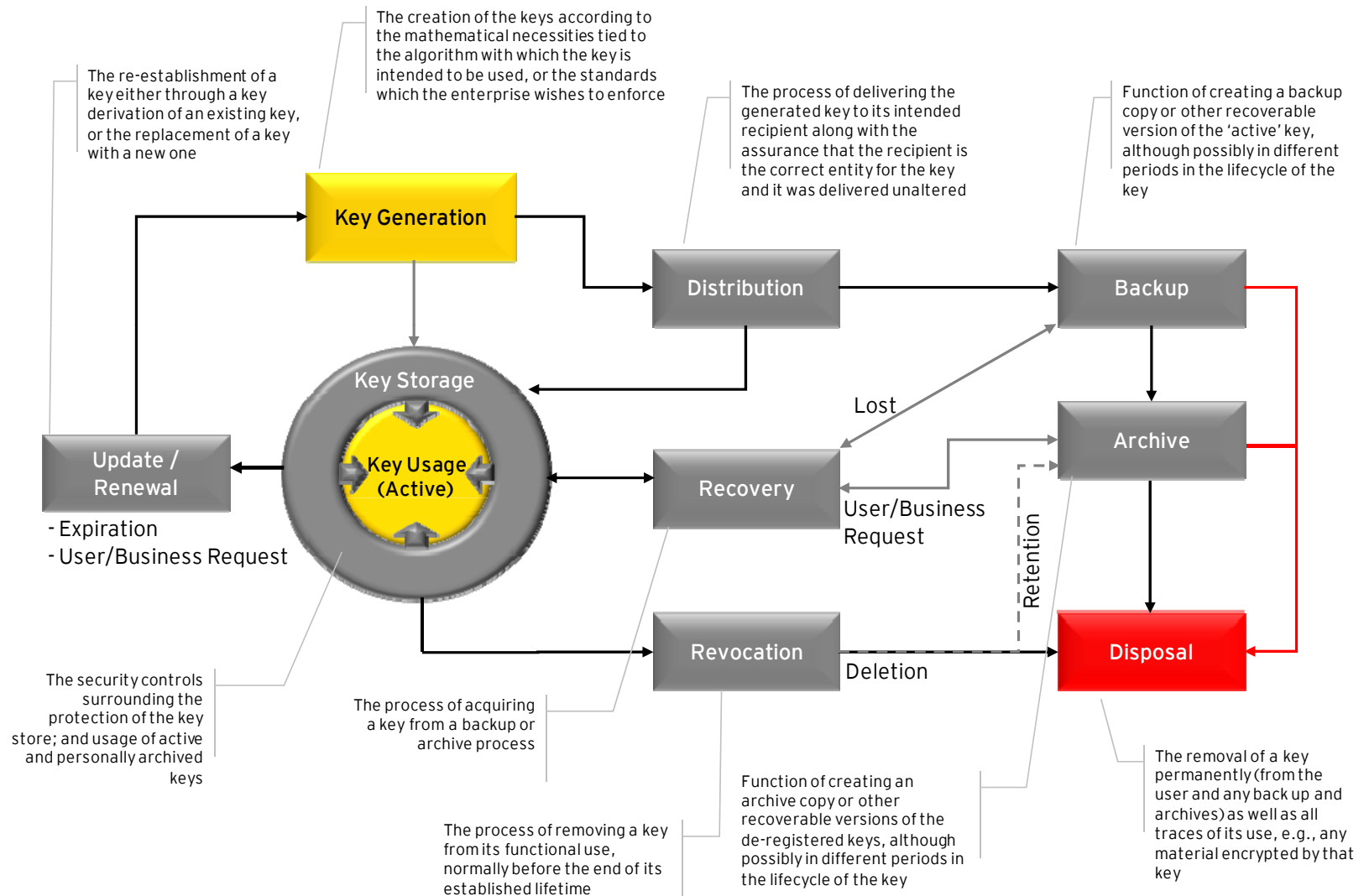
Of particular concern was the last item - measuring a program

Approached by a client to assist them in developing a methodology to review key management practices and provide a means of measuring improvement over time

Approach

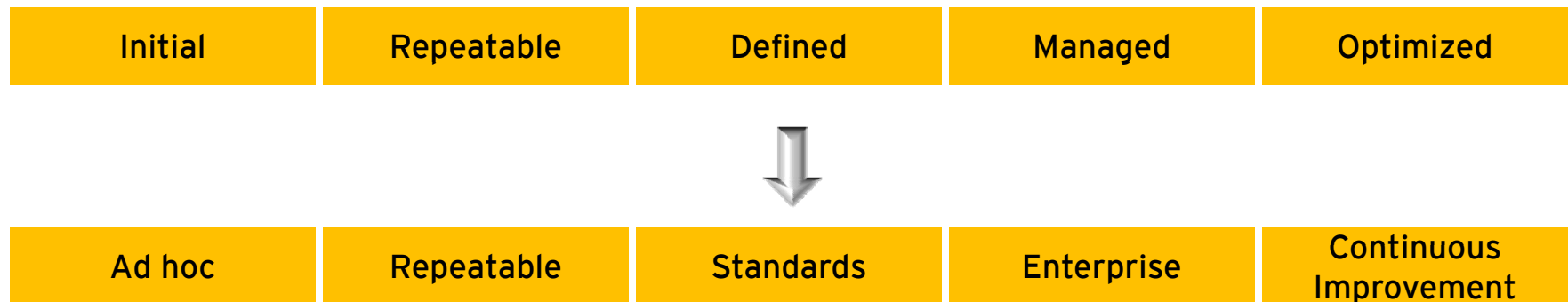


Key lifecycle management



Developing the model

- ▶ Started with capability maturity model as defined by Carnegie Mellon University (CMU)
- ▶ CMMs are great for process oriented maturity levels; not everything in key management was a perfect fit
- ▶ Started redefining maturity with a new concept



(we still used the traditional labels however)

Maturity model - generation

Generation – The creation of the keys (any type) according to the mathematical necessities tied to the algorithm with which the key is intended to be used, or the standards which the enterprise wishes to enforce

Level 1 - <i>Initial</i>	Level 2 - <i>Repeatable</i>	Level 3 - <i>Defined</i>	Level 4 - <i>Managed</i>	Level 5 - <i>Optimized</i>
<ul style="list-style-type: none"> ▶ Key generation is not controlled or managed ▶ Keys are generated inconsistently, often never the same way or with the same parameters 	<ul style="list-style-type: none"> ▶ Key generation is consistent within applications ▶ Differing applications may not use the same standards 	<ul style="list-style-type: none"> ▶ A standard, or multiple standards exist that applications and hardware security devices use to consistently generate strong keys in the environment ▶ Symmetric and asymmetric key generation standards are defined 	<ul style="list-style-type: none"> ▶ Standards are managed at the enterprise level ▶ Enterprise and localized applications use defined standards ▶ Applications are inventories and measured against compliance ▶ Technology implementation consistent with standards are used throughout all applications in the enterprise 	<ul style="list-style-type: none"> ▶ Continuous testing of applications to ensure compliance ▶ Processes are in place to evaluate, redefine and disseminate new standards for key generation ▶ Continuous evaluation of technology support for the enterprise is performed

Maturity model - distribution

Distribution – The process of delivering the generated key to its intended recipient along with the assurance that the recipient is the correct entity for the key and it was delivered unaltered

Level 1 - <i>Initial</i>	Level 2 - <i>Repeatable</i>	Level 3 - <i>Defined</i>	Level 4 - <i>Managed</i>	Level 5 - <i>Optimized</i>
<ul style="list-style-type: none"> ▶ Key distribution is not controlled or managed ▶ Key distribution is in-band and unencrypted ▶ Little to no authentication of the recipient is performed 	<ul style="list-style-type: none"> ▶ Key distribution is consistent within applications ▶ Recipients are authenticated before receiving a key ▶ Differing applications may not use the same standards; localized standards for distribution 	<ul style="list-style-type: none"> ▶ A standard, or multiple standards exist that applications use for consistent key distribution ▶ Symmetric and asymmetric key distribution are always mutually authenticated and secured 	<ul style="list-style-type: none"> ▶ Standards are managed at the enterprise level ▶ Enterprise and localized applications use defined standards consistently ▶ Technology implementation consistent with standards are used throughout all applications in the enterprise 	<ul style="list-style-type: none"> ▶ Continuous testing of applications to ensure compliance ▶ Processes are in place to evaluate, redefine and disseminate new standards for key distribution ▶ Continuous evaluation of technology support for the enterprise is performed

Maturity model - storage

Storage – The security controls surrounding the protection of the key store

Level 1 - <i>Initial</i>	Level 2 - <i>Repeatable</i>	Level 3 - <i>Defined</i>	Level 4 - <i>Managed</i>	Level 5 - <i>Optimized</i>
<ul style="list-style-type: none"> ▶ Key are stored insecurely ▶ Key storage is not controlled or managed ▶ Uncontrolled access to the key storage containers outside of the key holder 	<ul style="list-style-type: none"> ▶ Secure key storage is consistent within applications ▶ Access to key storage containers is controlled per individual application process ▶ Differing applications may not use the same standards; localized standards for key storage 	<ul style="list-style-type: none"> ▶ A standard, or multiple standards exist that applications use for consistent key storage ▶ Key storage containers are secured and distributed (transmitted) through defined and secure standards authenticating the recipient 	<ul style="list-style-type: none"> ▶ Standards are managed at the enterprise level ▶ Technology implementation consistent with standards are used throughout all applications in the enterprise ▶ Enterprise and localized applications use defined standards 	<ul style="list-style-type: none"> ▶ Continuous testing of applications to ensure compliance ▶ Processes are in place to evaluate, redefine and disseminate new standards for key storage ▶ Continuous evaluation of technology support for the enterprise is performed

Maturity model – backup / archive / escrow

Backup / Archive / Escrow – These functions involve creating a copy, or other recoverable version of the key, although possibly in different periods in the lifecycle of the key

Level 1 - <i>Initial</i>	Level 2 - <i>Repeatable</i>	Level 3 - <i>Defined</i>	Level 4 - <i>Managed</i>	Level 5 - <i>Optimized</i>
<ul style="list-style-type: none"> ▶ Key backup/archive/escrow (referred to as simply “backup”) not performed ▶ Key backup is not controlled or managed ▶ Uncontrolled access to the backup key outside of the key holder 	<ul style="list-style-type: none"> ▶ Key backup is consistent within applications ▶ Access to backup containers is controlled per individual application process ▶ Differing applications may not use the same standards; localized standards for backup 	<ul style="list-style-type: none"> ▶ A standard, or multiple standards exist that applications use for consistent key backup ▶ Backup containers are secured and distributed (transmitted) through defined and secure standards ▶ Integrated with overall key storage standards 	<ul style="list-style-type: none"> ▶ Standards are managed at the enterprise level ▶ Enterprise and localized applications use defined standards consistently ▶ Technology implementation consistent with standards are used throughout all applications in the enterprise 	<ul style="list-style-type: none"> ▶ Continuous testing of applications to ensure compliance ▶ Processes are in place to evaluate, redefine and disseminate new standards for key backup ▶ Continuous evaluation of technology support for the enterprise is performed

Maturity model – update / renewal

Update / Renewal / Expiration– The re-establishment of a key either through a key derivation of an existing key, or the replacement of a key with a new one

Level 1 - <i>Initial</i>	Level 2 - <i>Repeatable</i>	Level 3 - <i>Defined</i>	Level 4 - <i>Managed</i>	Level 5 - <i>Optimized</i>
<ul style="list-style-type: none"> ▶ Key are not updated or renewed, or not performed on a consistent basis ▶ Key update and renewal processes are not performed securely either in-band or out-of-band ▶ Little to no authentication of entity performing renewal or update ▶ Key do not have consistent or any expiration 	<ul style="list-style-type: none"> ▶ Secure update and renewal is consistent within applications ▶ Keys expire in a timely manner but without defined standards to guide them ▶ Key update and renewal processes authenticate the key holder performing the update/renewal ▶ Differing applications may not use the same standards; localized standards for key update and renewal 	<ul style="list-style-type: none"> ▶ A standard, or multiple standards exist that applications use for consistent key update and renewal ▶ Automated capabilities to perform update and renewal on behalf of users and applications 	<ul style="list-style-type: none"> ▶ Standards are managed at the enterprise level ▶ Technology implementation consistent with standards are used throughout all applications in the enterprise ▶ Enterprise and localized applications implement defined standards 	<ul style="list-style-type: none"> ▶ Continuous testing of applications to ensure compliance ▶ Processes are in place to evaluate, redefine and disseminate new standards for key update and renewal ▶ Continuous evaluation of technology support for the enterprise is performed

Maturity model – recovery

Recovery – Acquiring a key from a backup or archive process

Level 1 - Initial	Level 2 - Repeatable	Level 3 - Defined	Level 4 - Managed	Level 5 - Optimized
<ul style="list-style-type: none"> ▶ No recovery capability exists, or, only ad hoc user defined processes are implemented ▶ Existing ad hoc processes are not integrated with backup and/or archive 	<ul style="list-style-type: none"> ▶ Per application recovery processes are implemented ▶ Consistent only within application sets; inconsistent between applications ▶ Differing applications may not use the same standards; localized standards for key recovery ▶ Recovery management is user driven 	<ul style="list-style-type: none"> ▶ A standard, or multiple standards exist that applications use for consistent key recovery ▶ Recovery management is a defined set of processes with integrated access control of recovery keys, authentication of recovery manager, and secure distribution of recovered keys 	<ul style="list-style-type: none"> ▶ Standards are managed at the enterprise level ▶ Technology implementation consistent with standards are used throughout all applications in the enterprise ▶ Enterprise and localized applications implement defined standards 	<ul style="list-style-type: none"> ▶ Continuous testing of applications to ensure compliance ▶ Processes are in place to evaluate, redefine and disseminate new standards for key recovery ▶ Continuous evaluation of technology support for the enterprise is performed

Maturity model – revocation

Revocation – Removing a key from its functional use, normally before the end of its established lifetime

Level 1 - <i>Initial</i>	Level 2 - <i>Repeatable</i>	Level 3 - <i>Defined</i>	Level 4 - <i>Managed</i>	Level 5 - <i>Optimized</i>
<ul style="list-style-type: none"> ▶ Keys are not revoked upon compromise or loss, or, only ad hoc user defined processes are implemented ▶ Existing ad hoc processes are not integrated with recovery processes 	<ul style="list-style-type: none"> ▶ Per application revocation processes are implemented ▶ Consistent only within application sets; inconsistent between applications ▶ Differing applications may not use the same standards; localized standards for key revocation ▶ Revocation management is user driven 	<ul style="list-style-type: none"> ▶ A standard, or multiple standards exist that applications use for consistent key revocation ▶ Revocation management is a defined set of processes with integrated notification, key generation, and key distribution of new keys 	<ul style="list-style-type: none"> ▶ Standards are managed at the enterprise level ▶ Technology implementation consistent with standards are used throughout all applications in the enterprise ▶ Enterprise and localized applications implement defined standards 	<ul style="list-style-type: none"> ▶ Continuous testing of applications to ensure compliance ▶ Processes are in place to evaluate, redefine and disseminate new standards for key revocation ▶ Continuous evaluation of technology support for the enterprise is performed

Maturity model – disposal

Disposal – The removal of key permanently (from the user and any back up and archives) as well as all traces of its use, e.g., any material encrypted by that key

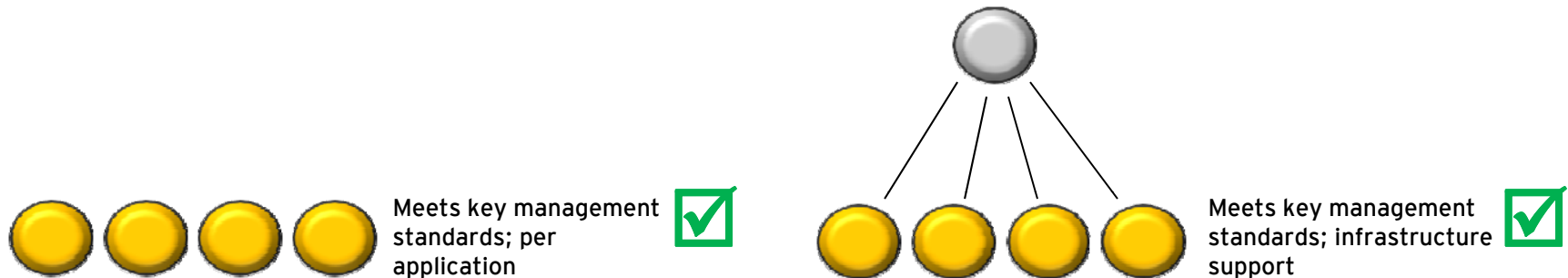
Level 1 - <i>Initial</i>	Level 2 - <i>Repeatable</i>	Level 3 - <i>Defined</i>	Level 4 - <i>Managed</i>	Level 5 - <i>Optimized</i>
<ul style="list-style-type: none"> ▶ Keys are not disposed of upon end of life, compromise or loss, or, only ad hoc user defined processes are implemented 	<ul style="list-style-type: none"> ▶ Per application disposal processes are implemented ▶ Consistent only within application sets; inconsistent between applications ▶ Differing applications may not use the same standards; localized standards for key disposal 	<ul style="list-style-type: none"> ▶ A standard, or multiple standards exist that applications use for consistent key disposal ▶ Removal of material encrypted by the key removed according to standards 	<ul style="list-style-type: none"> ▶ Standards are managed at the enterprise level ▶ Technology implementation consistent with standards are used throughout all applications in the enterprise ▶ Enterprise and localized applications implement defined standards ▶ Removal of material encrypted by the key removed consistently throughout the enterprise 	<ul style="list-style-type: none"> ▶ Continuous testing of applications to ensure compliance ▶ Processes are in place to evaluate, redefine and disseminate new standards for key disposal ▶ Continuous evaluation of technology support for the enterprise is performed

Applying the model

- ▶ Client wanted an examination of seven solutions; Applied model per solution
 - ▶ PKI
 - ▶ VPN
 - ▶ SSL management
 - ▶ Secure email
 - ▶ FDE
 - ▶ Tape backup
 - ▶ SFTP
- ▶ Interview application/solution owners; key managers
 - ▶ Discussion / documentation
 - ▶ Understand what is implemented
- ▶ Map implementation to maturity level, all phases
- ▶ Needed an additional parameter
 - ▶ **Effectiveness**
 - ▶ E.g., a 'standard' may say to use 56 bit DES, however, the effectiveness of that standard is unacceptable

Moving from 3 to 4

- ▶ Initially difficult to define



- ▶ Consensus centered around 2 elements
 1. Reduction in implementation (technology) of standards
 2. Gain in automation (efficiency)
- ▶ Moving from 3 → 4 needed to address two things
 1. Is the associated cost (app and resources) worth the investment?
 2. Is there even a technology available to make it happen?

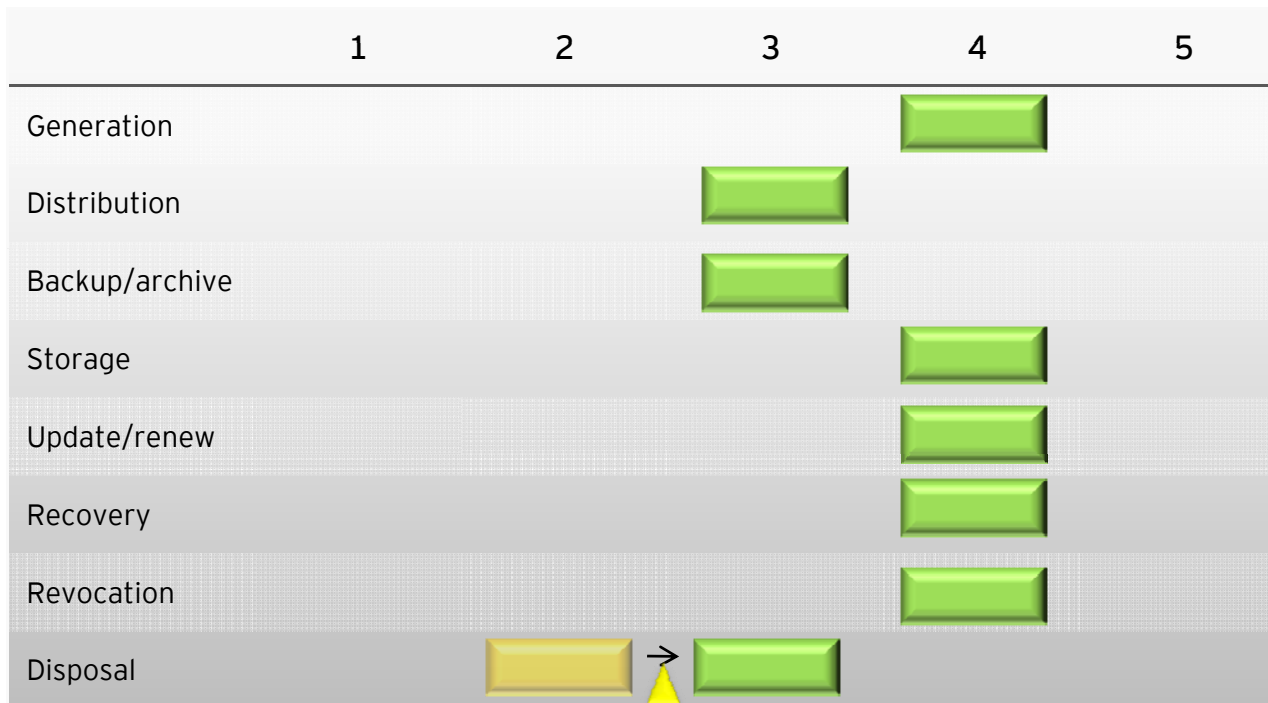
Applying the model

Public key infrastructure (PKI) solution

	1	2	3	4	5
Generation				■	
Distribution			■		
Backup/archive			■		
Storage				■	
Update/renew				■	
Recovery				■	
Revocation				■	
Disposal		■			

Applying the model – remediation areas

Public key infrastructure (PKI) solution



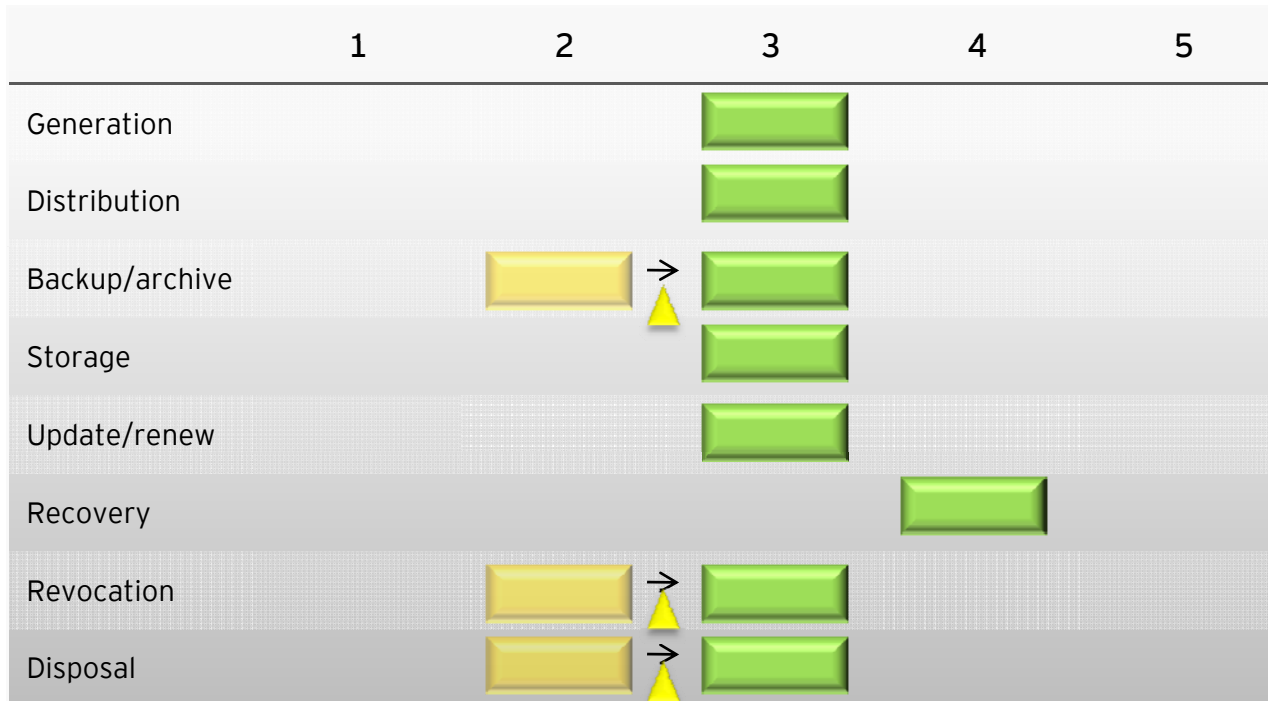
Applying the model

Full disk encryption (FDE) solution

	1	2	3	4	5
Generation			■		
Distribution			■		
Backup/archive		■			
Storage			■		
Update/renew			■		
Recovery				■	
Revocation		■			
Disposal		■			









Applying the model – remediation areas

Full disk encryption (FDE) solution



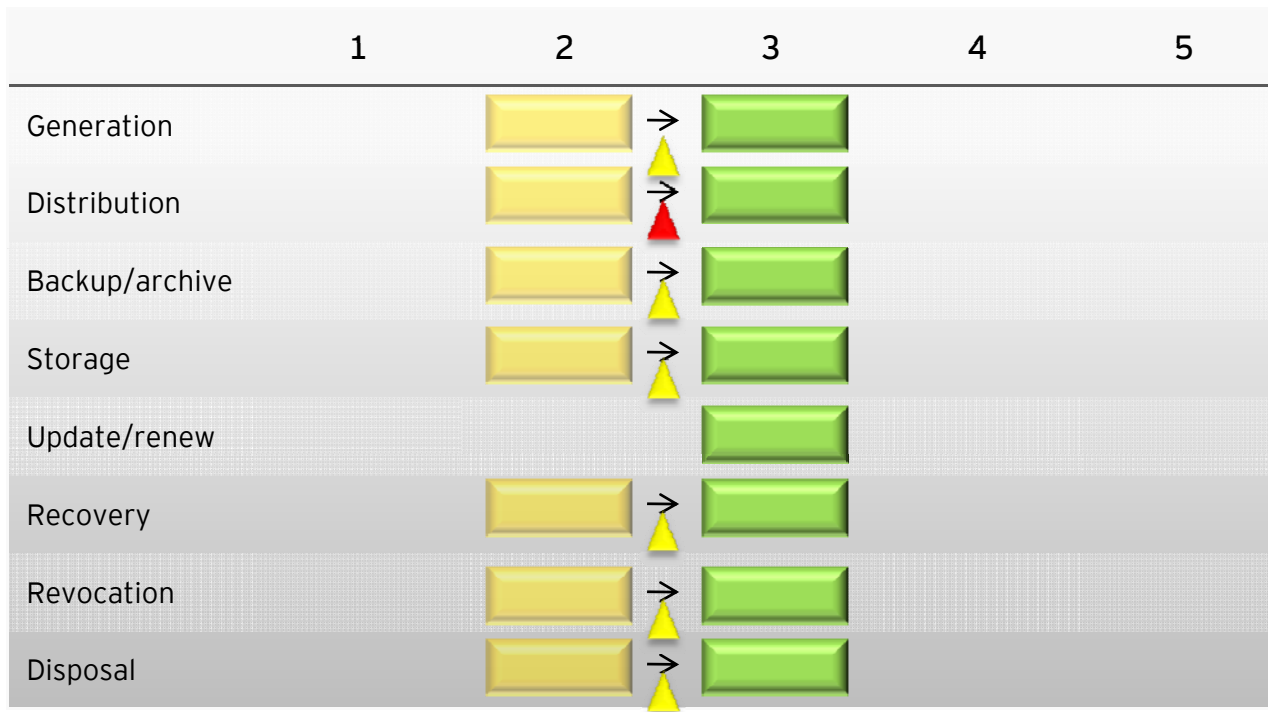
Applying the model

SSL certificate and key management











	1	2	3	4	5
Generation					
Distribution					
Backup/archive					
Storage					
Update/renew					
Recovery					
Revocation					
Disposal					

Applying the model – remediation areas

SSL certificate and key management



Risk analysis of results - dashboard

	Current State	Future State	Remediation	Duration	Cost
PKI			X	1-3 mo	\$
FDE			X	2-4 mo	\$\$
Tape backup			X	1-3 mo	\$
VPN			X	6-8 mo	\$\$
SSL			X	6-8 mo	\$\$
Secure email			X	8-10 mo	\$\$\$
SFTP					

Remediation roadmap created for each area needing improvement

Gaps and lessons learned

Creating a maturity model addressing only the phases of key lifecycle management was not enough



The model allowed us to examine how individual applications managed keys

- Website SSL keys and certificates
- Endpoint (laptop) encryption
- Secure email
- Tape backup encryption
- Secure file transfer
- Secure VPN for remote access



What was missing

- Policies and standards
- Roles, responsibilities and ownership issues
- Compliance

Governance

Gaps and lessons learned

- ▶ The model provided less value than anticipated
 - ▶ What we learned: *It's okay to be a 3*
- ▶ Standards, and adherence to those standards was the most significant aspect of good key management
- ▶ Recommendation in the end



Questions

▶ ?

Contact

- ▶ Chris Kostick
Executive Director
christopher.kostick@ey.com
410-783-3838