Phase 1: Writing Good Guidance

Introduction

- Creating contents of guide
- Deciding…
  - What to recommend
  - How to structure the guide
  - How to write recommendations and supporting data clearly
- MITRE developed procedures that support creating guidance efforts

How do you know what to recommend?

Focus on areas of impact to product users

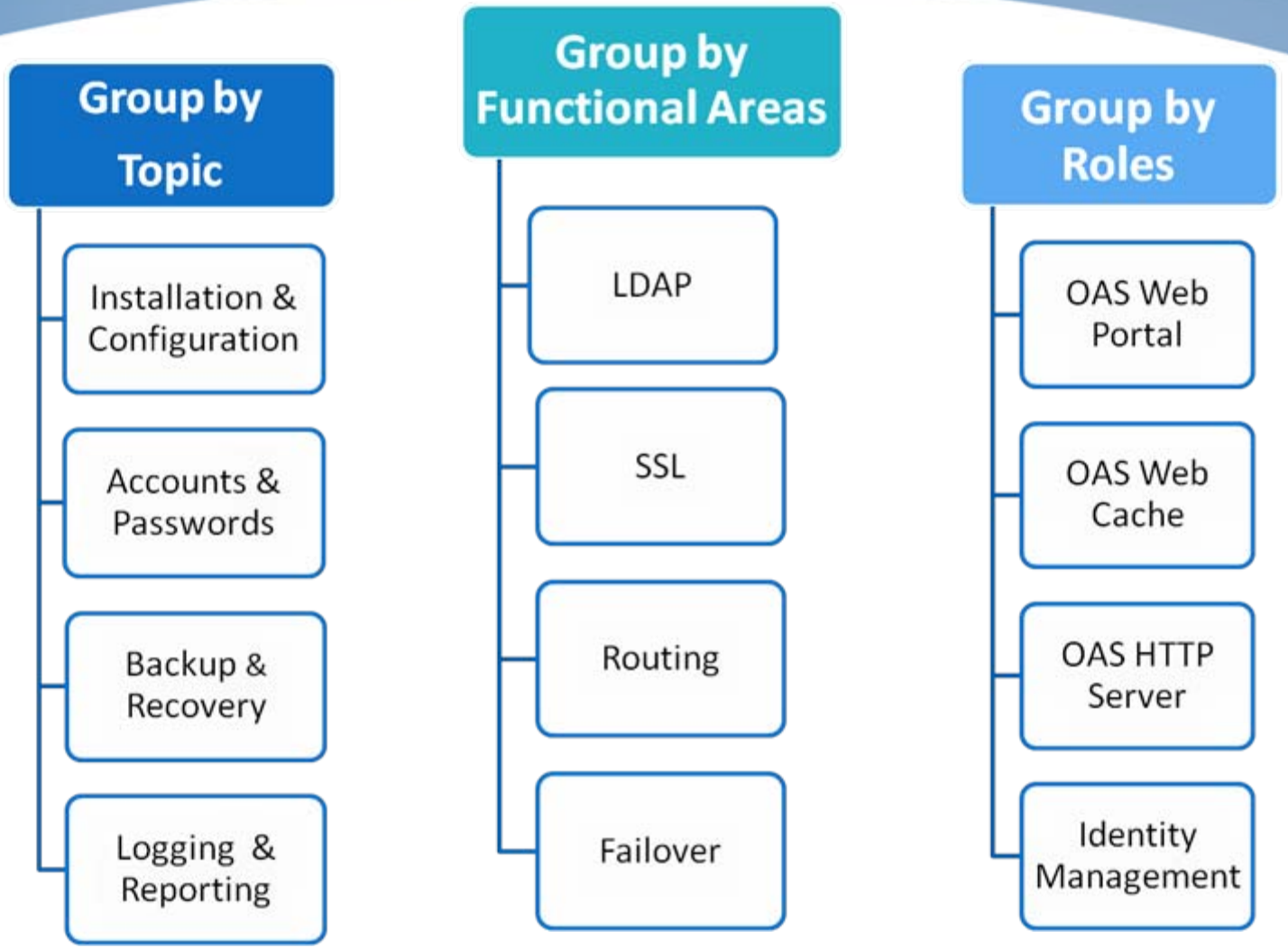
- Deployment options
- Installation and configuration
- Accounts and Passwords
- Security features
- Product key features

Potential threats associated with type of product

- Expected product usage
- Services product provides / does not provide
- Documented attacks against prior versions of product helps to understand possible threats

MITRE

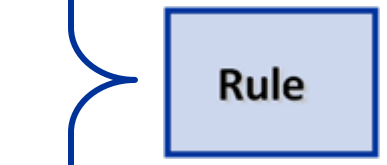
Structure Guide Content



MITRE

Create

Recommendation	**What** security-relevant action to take
Rationale	**Why** the action should be taken
How To	**How** to carry out the action
Compliance Check (Optional)	Discussed in Investigate phase



Create -> Rule

Recommendation: What
Rationale: Why
How To: How

- Users should change their passwords often
- Limit access to the Oracle Application Server configuration files
- Set the “log_trace” control in the msd.conf file to record necessary messages
- Restrict access to the C:\Windows folder for non-authenticated users

These are examples of poorly worded recommendations

What do Administrators Need?

Recommendations that are:

- Unambiguous
- Clear and concise
- Directive (imperative form)
- Measurable, if possible

How does MITRE address these needs when it creates content?

Create -> Rule

Recommendation: What
Rationale: Why
How To: How

Writing Style Guidelines

- Always use imperative voice (Enable screen saver)
- Put the word “only” close to the word(s) it modifies
- Do not use the words “restrict” or “limit”

Imperative Voice

Imperative voice is direct and clearly states that an action is taken. Passive voice is weaker and wordier.

For example:

Do not say “It is recommended that the NSA guide on Windows Server 2003 be applied.”

Do say “Apply the NSA guide on Windows Server 2003.”

Only

Putting “only” at a distance from the word it modifies often creates an ambiguous statement.

For example:

If you want to say that only administrators should have read access to the C:\Windows folder:

Do not say “Only allow read access on the C:\Windows folder for administrators.”

Do say “Allow only administrators to have read access to the C:\Windows folder.”

Restrict & Limit

"Restrict" and "limit" often make the sentence in which they appear ambiguous. They are too vague. Be specific.

For example:

"Restrict access to the C:\Windows folder for non-authenticated users."

- Only non-authenticated users have access to the C:\Windows folder.
- Non-authenticated users have some access to the C:\Windows folder.
- Non-authenticated users have access to only the C:\Windows folder.

Do say "Allow only authenticated users to have access to the C:\Windows folder."

Create -> Rule

Recommendation: What
Rationale: Why
How To: How

Ambiguous	Unambiguous
Users **should change** their passwords **often**.	Set the “Password Expiry Time” control to 90 days.
Set the “log_trace” control in the msd.conf file to record **necessary** messages.	Set the “log_trace” control in the msd.conf file to record all ACL, ADMIN, CONFIG, and SSL messages.
Restrict access to the C:\Windows folder for non-authenticated users.	Allow only administrators to have access to the C:\Windows folder.

Writing Style Guidelines

MITRE

Example 1: Windows XP Password Recommendation

"Use strong passwords."

- Separate high level recommendation into parts that are
  - unambiguous
  - clear and concise
  - directive
  - measurable

Example 1: Windows XP Password Recommendation

"Use strong passwords."

- Password age
  - Minimum password age
  - Maximum password age
- Password length
- Password complexity
- Password history
  - Minimum password length
  - Maximum password length

Set the 'minimum password length' control to at least '12' characters.

Create Rationale

Recommendation	What security-relevant action to take
Rationale	**Why** the action should be taken
How To	How to how to carry out the action
Compliance Check (Optional)	Discussed in Explore phase

Create -> Rule

Recommendation: What
Rationale: Why
How To: How

Model for Rationales

1. States what the control is and does
2. States the default value for the control
3. Explains the impact of not implementing the recommendation
4. Indicates the impact of following the recommendation, if appropriate

Recommendation: "Change the default encryption key during the installation of the Tivoli Identity Manager."

"The encryption key is used to encrypt TIM passwords and other sensitive data. The default encryption key is [sunshine]. If the default encryption key is not changed a malicious user could potentially use the default key to gain access to TIM passwords and sensitive data. Changing the default encryption key will help protect Tivoli passwords and sensitive data."

MITRE

Example 2: Rationale for Minimum Password Length

Set the 'minimum password length' control to at least '12' characters.

1. States what the control is and does
2. States the default value for the control
3. Explains the impact of not implementing the recommendation
4. Indicates the impact of following the recommendation, if appropriate

The ‘minimum password length’ control sets the minimum number of characters required in a password. The default value is 6. Not implementing this recommendation could result in passwords that are easily guessed. Conversely, setting the ‘minimum password length’ control to at least 12 creates lengthy passwords which increases the risk of passwords being forgotten or written down.

Create How To

Recommendation	What security-relevant action to take
Rationale	Why the action should be taken
How To	**How** to how to carry out the action
Compliance Check (Optional)	Discussed in Explore phase

Create -> Rule

Recommendation: What
Rationale: Why
How To: How

Example: “Enable SSL for Web Applications.”

How To:

1. Log in to Central Administration.
2. Navigate to Application Management > SharePoint Web Application Management.
3. Select Create or extend Web application.
4. Select Create a new Web application if creating a new application, or Extend an existing Web application if extending an existing application.
4.1. If extending an existing Web application, select the appropriate Web application.
5. Navigate to Security Configuration > Use Secure Sockets Layer (SSL).
6. Select the option [Yes].
7. Enter other options with values appropriate to the deployment.
8. Select OK.

Create -> Rule

Recommendation: What
Rationale: Why
How To: How

Example:

“Use Microsoft Internet Explorer 6.x or later to access Central Administration.”

How To:

Self-explanatory.

Create -> Rule

Recommendation: What
Rationale: Why
How To: How

Example:

"Apply the security guidance for Internet Explorer 7 found at the NIST National Vulnerability Database checklist site."

How To:

Self-explanatory. For more information refer to the NIST website: http://nvd.nist.gov/ncp.cfm and select the "Checklist Repository" link.

Example 3: How To for Minimum Password Length

- Launch the "Local Security Settings" editor
  - **Start -> Run -> "secpol.msc"**
- Navigate to the "Password Policy" group
  - **Security Settings -> Account Policy -> Password Policy**
- Double-click the "Minimum password length" policy
- Set the "Password must be at least:" value to 12

Completed Example

Recommendation:

Set the 'minimum password length' control to at least '12' characters.

Rationale:

The ‘minimum password length’ control sets the minimum number of characters required in a password. The default value is 6. Not implementing this recommendation could result in passwords that are easily guessed. Conversely, setting the ‘minimum password length’ control to at least 12 creates lengthy passwords which increases the risk of passwords being forgotten or written down.

How To:

1. Launch the "Local Security Settings" editor
    - Start -> Run -> "secpol.msc”
2. Navigate to the "Password Policy" group
    - Security Settings -> Account Policy -> Password Policy
3. Double-click the "Minimum password length" policy
4. Set the "Password must be at least:" value to 12

MITRE

Create Recap

RULE

Recommendation	**What** security-relevant action to take	Writing Style Guidelines
Rationale	**Why** action should be taken	Model for Rationales
How To	**How** to carry out the action	Steps for Admin to follow

Recommendation Tracker tool

Recommendation Tracker

Recommendation Tracker Goal

Facilitate **consistent** guidance authoring through an established **standardized format** for **creating**, **developing**, and **tracking** all information pertinent to security guide and benchmark generation.

Codifies a proven guidance creation process.

https://sourceforge.net/projects/rectracker/

What does the RT do?

Provides structure to the guidance development process

- Clearly breaks out all key components to a Rule
- Leads users in a step-by-step fashion to produce clear guidance

Supports team collaboration

- User roles and task assignment
- Comments on key components
- Progress tracking

Enables offline development with synchronization

- Allow users to work in their environment of choice
- Facilitate team collaboration

Enables users to output guidance in standardized formats

- No additional burden to use standards

https://sourceforge.net/projects/rectracker/

MITRE

Demo: Recommendation Tracker

Exercise 4: Recommendation Tracker

- Let's add the new minimum password length rule to the 'Microsoft Windows XP' guide
- Demo version of the RT can be found here
  - C:\BDCTools\rt\RTClient.jar
- Log in as:
  - Username: 'bsmith'
  - Password: 'password'

Exercise 4: RT Continued

- Populate the following fields
  - Title
  - Recommendation
  - Rationale
    - Impact if not followed
- Be sure to save...

Extra Credit:

- Correct the "Guest account status" rule.