NIST Cybersecurity White Paper
NIST CSWP 32 ipd

NIST Cybersecurity Framework 2.0:
A Guide to Creating Community Profiles

Initial Public Draft

Cherilyn Pascoe
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Julie Nethery Snyder
The MITRE Corporation

Karen Scarfone
Scarfone Cybersecurity

February 26, 2024

1 Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this
2 paper in order to specify the experimental procedure adequately. Such identification does not imply
3 recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or
4 equipment identified are necessarily the best available for the purpose.

12 **Author ORCID iDs**
13 Cherilyn Pascoe: 0009-0009-6216-4864
14 Julie Snyder: 0009-0004-6352-2831
15 Karen Scarfone: 0000-0001-6334-9486

16 **Public Comment Period**
17 February 26, 2024 – May 3, 2024

18 **Submit Comments**
19 framework-profiles@nist.gov
20
21 National Institute of Standards and Technology
22 Attn: Applied Cybersecurity Division, Information Technology Laboratory
23 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

24 **Additional Information**
25 Additional information about this publication is available at
26 https://csrc.nist.gov/pubs/cswp/32/a-guide-to-creating-csf-20-community-profiles/ipd, including related content,
27 potential updates, and document history.

28 **All comments are subject to release under the Freedom of Information Act (FOIA).**
29

30 Abstract

31 The NIST Cybersecurity Framework (CSF) 2.0 introduced the term "Community Profiles" to
32 reflect the use of the CSF for developing use case-specific cybersecurity risk management
33 guidance for multiple organizations. This guide provides considerations for creating and using
34 Community Profiles to help implement the Framework. The guide describes Community
35 Profiles, provides guidance for the content that may be conveyed through a Community Profile,
36 and offers a Community Profile Lifecycle (Plan, Develop, Use, Maintain).

37 Keywords

40 Audience

41 The primary audience for this guide is communities, which are groups of organizations with
42 shared interests in cybersecurity risk management within a specific context, such as a sector,
43 technology, or challenge, that are interested in developing one or more Community Profiles.

44 Supplemental Content

45 The NCCoE has worked with communities to develop Community Profiles for a variety of use
46 cases. These Community Profiles are available on the NCCoE Framework Resource Center.
47 Communities that are interested in working with the NCCoE to develop Community Profiles and
48 supporting resources or that have suggestions for improving this guide may contact the NCCoE
49 at framework-profiles@nist.gov or visit the NCCoE Framework Resource Center.

50 Acknowledgments

57

58 **Table of Contents**

69 **List of Tables**

71 **List of Figures**

74

75 **Preface**

76 Since the NIST Cybersecurity Framework (CSF) was first released in 2014, the CSF has been used
77 by communities with shared interests in cybersecurity risk management. These communities
78 developed what are now called "Community Profiles" to outline shared interests, goals, and
79 outcomes within a specific context, such as a sector, technology, or challenge. CSF 2.0
80 introduced the term "Community Profiles" to describe the ways various organizations have
81 used CSF Profiles to develop cybersecurity risk management guidance that applies to multiple
82 organizations, as well as to differentiate them from Organizational Profiles that are internally
83 focused on the organization itself and generally not shared publicly. A Community Profile can
84 be thought of as guidance for a specific community that is organized around the common
85 taxonomy of the CSF.

86 This guide provides considerations for creating and using Community Profiles to implement the
87 CSF 2.0. This guide is intended to provide a starting point, as there are a myriad of ways that
88 Community Profiles have been developed to serve communities. Communities can build on the
89 ideas in this guide to create a Community Profile that supports their needs where they share
90 common priorities.

91 **1. About Community Profiles**

92 A *Community Profile* describes shared interests, goals, and outcomes for reducing
93 cybersecurity risk among a number of organizations. Community Profiles provide a way for
94 communities to reflect a consensus point of view about cybersecurity risk management.
95 Organizations in the community can use a Community Profile as the basis of, or to inform, their
96 Organizational Target Profiles. Some communities may develop more than one Community
97 Profile, based on the scope of their needs.

98 *Communities* are organizations that share a common context and an interest in their
99 cybersecurity posture. Examples of communities that a Community Profile may support include:

100 • Sectors/subsectors (e.g., critical infrastructure sectors)

101 • Technologies (e.g., mobile, cloud)

102 • Other use cases (e.g., thwarting ransomware attacks)

103 Figure 1 provides an abstract view of Community Profiles, which use the CSF 2.0 Core to identify
104 and prioritize cybersecurity outcomes that are necessary to meet the community's priorities.
105 Community priorities influence the CSF 2.0 outcomes that are prioritized. The stars in Fig. 1
106 represent the degree of importance of CSF 2.0 outcomes in the context of the Community
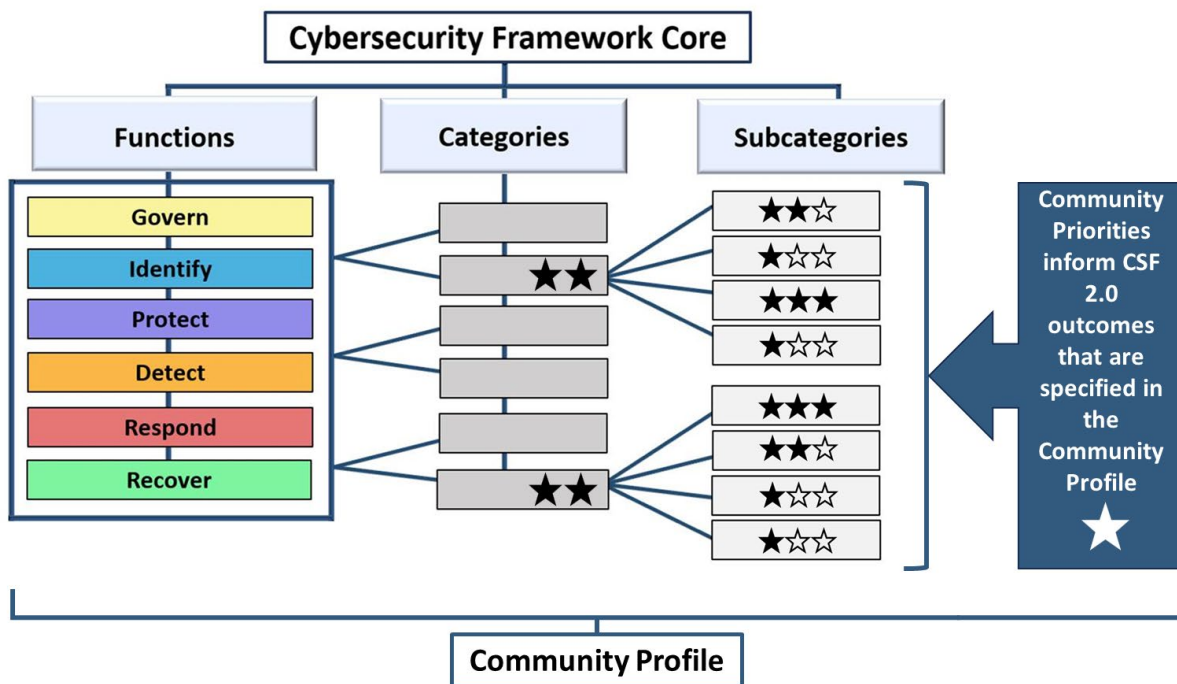107 Profile.

109 **Fig. 1. Representation of Community Profiles Using the CSF Core.**

110 Examples of Community Profiles are available on the [NCCoE Framework Resource Center](#). Once
111 available, NIST will add Community Profiles that are developed for CSF 2.0 to the NCCoE
112 Framework Profiles Resource Center.

1.1. Benefits

114 Community Profiles offer a variety of potential benefits, including:

115 • Describing a shared taxonomy for cybersecurity risk management and priorities in the
116   context of the community

117 • Encouraging common target outcomes that organizations within the community can use
118   to inform their assessments of cybersecurity progress

119 • Aligning requirements from multiple sources under one framework

120 • Leveraging expertise across the community

121 • Minimizing the burden for each organization by providing priorities and outcomes that
122   organizations can use to develop their own Target Profiles

123 The benefits communities will find most valuable shape how they scope and approach
124 developing their Community Profile(s).

1.2. Developers and Owners

126 Efforts to develop Community Profiles encourage collaboration across the community — often
127 the efforts to bring a community together to develop a Community Profile to find consensus are
128 just as valuable as the publication. The Community Profile developer should have community
129 expertise, capabilities to convene other experts that represent the interests of the community,
130 and resources to support development. Examples of organizations that may collaboratively
131 develop and maintain Community Profiles include trade associations, nonprofit entities,
132 government agencies, advisory committees, and information sharing organizations. A large
133 organization with distinct operational components might even develop a Community Profile for
134 internal use across its divisions or units.

135 **2. Community Profiles Contents**

136 Community Profiles use the CSF Core to highlight and prioritize cybersecurity outcomes that are
137 important for achieving community priorities. A Community Profile provides information that
138 enables the community to make risk-informed decisions when determining how to use its
139 cybersecurity resources.

140 Community Profiles align community priorities with outcomes from the CSF 2.0 Core by
141 specifying Subcategories as "included" in the Community Profile. As depicted in Table 1,
142 Community Profiles should include:

143 • The ***priority*** level of each CSF 2.0 outcome (e.g., ranking 1, 2, 3, or Low/Moderate/High),

144 • A ***rationale*** for the priority level(s) to help users understand applicability of the CSF 2.0
145 outcome in the context of the community (e.g., an explanation of community-specific
146 challenges or threats that the outcome will help the community address), and

147 • Applicable ***Informative References/Mappings*** that can help users achieve the CSF 2.0
148 outcomes or that can inform assessments of outcomes their organization is already
149 achieving (e.g., industry standards or guidelines).

150

CSF 2.0 Outcome		Priority	Rationale	Informative References / Mappings
ID.AM-01	Inventories of hardware managed by the organization are maintained			
ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained			

151 **Table 1 Sample Community Profile Template**

152 Communities may also choose to include:

153 • **Considerations** – Supplements the rationale by providing additional recommendations,
154 explanations, or other supporting details for a CSF 2.0 outcome within the context of
155 this Profile

156 • **Implementation Examples** - Provides one or more examples of implementation
157 activities that could be implemented to achieve part or all of the CSF 2.0 outcome

158 • **Notes** – Offers any additional details about a CSF 2.0 outcome within the community's
159 context, such as notes to Community Profile users

160 Communities may wish to further elaborate on how CSF 2.0 outcomes help them address more
161 discrete priorities and objectives. For example, priority levels, considerations, and
162 implementation examples may differ for one community priority in comparison to another.

163

164   **Using Crosswalks and Mappings for Community Profiles**

165   Communities may have requirements from a variety of laws,
166   regulations, standards, and other resources. Mappings provide a way of
167   identifying and describing relationships of these many resources.
168   Mappings to the NIST CSF 2.0 and other NIST publications are stored in
169   the Cybersecurity Privacy and Reference Tool (CPRT).
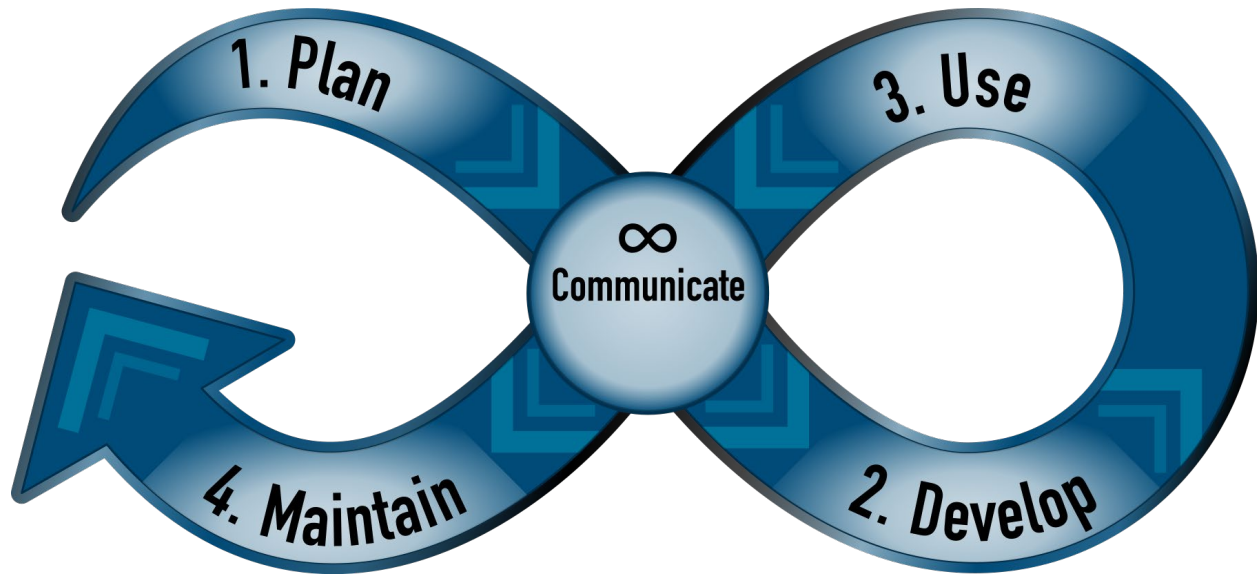
170   **3. The Community Profile Lifecycle**

171

172   <center>**Fig. 2: Community Profile Lifestyle**</center>

173   Fig. 2 illustrates the Community Profile Lifecycle. Developing a Community Profile begins with a
174   **planning** process that includes understanding the needs of the community it is intended to
175   support and determining the scope of the Profile. Thoughtful planning enables the
176   **development** process, resulting in the Community Profile. The Profile is then ready for **use** by
177   organizations in the community. Community Profiles are reviewed periodically and updated as
178   needed to ensure they are adequately **maintained** and continue to meet the needs of the
179   community or are retired when no longer needed.

180   A thread of communication runs throughout the Community Profile Lifecycle. Coordination and
181   collaboration among organizations within the community helps develop a Community Profile
182   that is realistic and useful throughout its lifespan.

183   The section below provides a summary of the Community Profile Lifecycle phases.

184 <u>**Summary of Community Profile Lifecycle Phases**</u>

1: Plan	2: Develop	3: Use	4: Maintain
Audience: determine the community	**Prioritize:** identify community priorities and objectives	**Collaborate and Coordinate:** determine how to use the Community Profile most effectively within organizations and across the community	**Measure Impact:** evaluate the success of the Community Profile and identify additional needs
Scope: determine what the Community Profile will address	**Align:** align community priorities to CSF cybersecurity outcomes	**Assess:** determine the current state of the community and organizations	**Monitor/Feedback:** determine if changes are needed to make the Profile more effective for the community
Participants: determine who will contribute to development	**Document:** complete the Community Profile with relevant content		**Update:** adjust Community Profile content as needed
References: identify community-specific standards, regulations, and other resources	**Feedback:** engage the community to provide feedback		**Retire:** retire the Community Profile when no longer needed
Content: determine what to include in the Community Profile	**Inform:** notify the community that the Profile is available and ready for use		

185   **Communicate (All Phases)**
186   Communication throughout the lifecycle helps the community develop an appropriate Community
187   Profile.

188   **3.1. Plan**

189
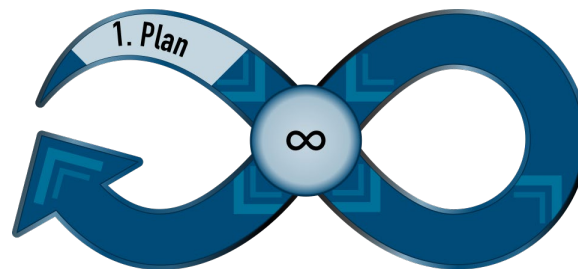
190   When planning the creation of a Community Profile, perform these actions:

191   1. **Identify the intended audience for the Community Profile.** Determine whether the
192   Profile is intended for the entire community or specific parts of or roles within the
193   community. Most Community Profiles are intended to address many roles, from
194   directors and executive leaders to hands-on implementers.

195 2. **Scope the Profile.** The Profile's scope should be broad enough to accommodate the
196 variety of community members but not so broad that it does not adequately capture the
197 community's cybersecurity needs. Some communities also determine whether the
198 Community Profile will be a voluntary resource or will be required for the community.

199 3. **Identify participants in the development process.** Aligning community priorities
200 requires participation of knowledgeable experts across the community with a variety of
201 operational experience in addition to cybersecurity experts. Participants should be
202 willing to participate throughout the Profile development process and will ideally
203 champion its use once the Profile is complete.

204 4. **Identify community-specific Informative References.** *Informative References* are
205 standards, guidelines, regulations, and other resources to help inform how a community
206 achieves the outcomes in the CSF Core. Communities should take advantage of context-
207 specific regulations, relevant sector/technology-specific standards, industry best
208 practices, and other available references that can support development and use of the
209 Community Profile. These can be mapped to outcomes in the CSF. Communities may
210 incorporate available references, including available CSF mappings, to aid practitioners
211 in using the Profile.

212 5. **Decide what to include in the Profile.** At a minimum, a Community Profile indicates
213 which CSF Functions, Categories, and Subcategories align with community priorities.
214 This helps indicate which cybersecurity activities and outcomes are most supportive to
215 community objectives, operational functions, and other priorities. A Community Profile
216 may also provide discussions of priorities and implementation guidance.

217

218 The state of the community that will be served by the Profile (e.g., cybersecurity
219 knowledge and maturity) can inform decisions regarding what type of information to
220 include and the necessary level of detail. Each community determines the appropriate
221 level of detail to communicate and the effective structure of the document (e.g.,
222 content that appears in the main body vs. an appendix).

223 **Integrating Other NIST Frameworks**

224 While a CSF Community Profile can be a valuable tool on its own,
225 communities may consider integrating other related or complementary
226 frameworks, such as the [NIST Privacy Framework](#), [NIST (cybersecurity)](#)
227 [Risk Management Framework (RMF)](#), or [NIST Artificial Intelligence (AI)](#)
228 [RMF](#). Additionally, incorporating links to other resources, such as the
229 [NICE Workforce Framework for Cybersecurity (NICE Framework)](#) or [NIST](#)
230 [Privacy Workforce Taxonomy](#), may help communities with identifying
231 work roles and aligning staff to implement prioritized Subcategories in
232 the Community Profile.

233   **3.2. Develop**

234
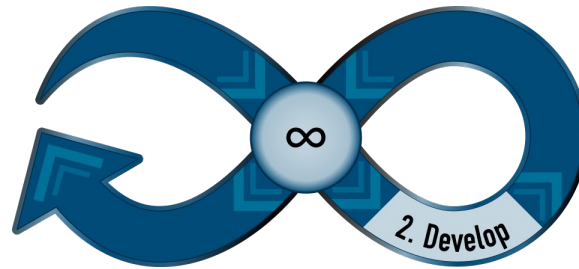
235   After planning a Community Profile, follow these steps to develop it:

236   1. **Identify community priorities and objectives.** While each organization within a
237   community has its own mission objectives and priorities, there are common or universal
238   interests that support the community. Community Profile teams begin with identifying
239   these universal priorities, which describe the fundamental purposes, operations, or use
240   cases of a community.

241   Questions to ask that may help the community identify its shared priorities include:

242   • How would you describe the purpose of the community?

243   • What are the critical activities in the community and why are they important?

244   • What are the current risk management requirements the community must
245   adhere to?

246   • Are there current community opportunities or priorities to include?

247   • Are there any dependencies outside the community?

248   • What are the threats to the success of the community?

249   • What are the key assets that support each priority?

250   • What are the risk appetite statements of the community?

251   • What assessment criteria should be used?

252   Once the priorities are agreed upon, the community may decide to rank the priorities in
253   order of relative importance. This helps organizations within the community make
254   strategic planning decisions.

255   2. **Align community priorities with CSF outcomes.** Once community priorities are
256   identified, the development team aligns those priorities with the CSF outcomes that
257   enable or support them. Communities can choose a simple prioritization schema (e.g.,
258   Included/Not Included) or a multi-level schema (e.g., High, Moderate, Implement Later)
259   to provide more insights when creating a gap analysis or action plan. Inputs for adding
260   and prioritizing outcomes include community-specific Informative References, shared
261   threats in the community, inputs from community experts, and other resources that the
262   community finds beneficial.

263 3. **Fill out the Profile.** There is no required format for a Community Profile. Some
264   communities use a narrative format with prose and tables. Others prefer a table format
265   that can be manipulated and sorted in a variety of ways. Still others prefer a format that
266   can be ingested into and manipulated by governance tools.

267   Development teams can capitalize on existing resources rather than creating the
268   Community Profile from a virtual blank page. For example, some communities may
269   already have a set of priorities or community-specific cybersecurity standards.

270   Also, the NIST National Cybersecurity Center of Excellence (NCCoE) has published
271   multiple Community Profiles that can be used as examples of additional narrative
272   discussions that may be included along with the basic Community Profile contents
273   described in Section 2. Published Community Profiles are available on the NCCoE
274   Framework Resource Center.

275 4. **Engage the community to provide feedback.** Engaging the community for feedback is a
276   critical part of developing an effective Community Profile and increases the likelihood
277   that the Profile will be accepted and used by organizations in the community. The
278   development team may wish to engage the community at multiple milestones during
279   development. At a minimum, once the development team has completed the draft
280   Community Profile, it should seek input from the broader community and incorporate
281   any feedback that will help the Profile be used successfully.

282 5. **Inform the community when the Profile is finalized.** The final Community Profile should
283   be hosted by the community in a location that all community members can access. The
284   community should promote the Profile to its members so they know it is available for
285   use (for example, an email to members or social media announcements).

286 ## 3.3. Use

287
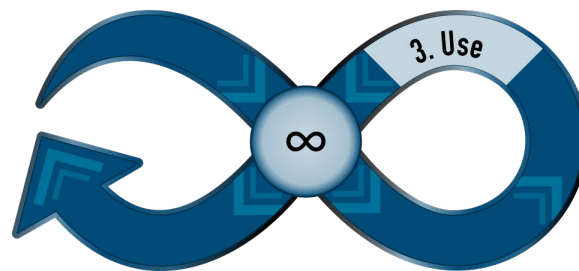
288 Community Profiles provide a shared view of cybersecurity that facilitates collaboration and
289 coordination throughout the community. It is easier for communities to share information
290 when community members are each starting with a shared way of discussing the topic.

291 Examples of how organizations can use Community Profiles include:

292 • Inform executive leadership of community-level cybersecurity expectations and goals

293 • Align business and operational practices with supporting cybersecurity activities that
294   have been vetted by the community

295 • Benchmark against community expectations when developing the organization's
296   Organizational Current Profile

297 • Inform the organization's Target Profile(s) or use it as the organization's Target Profile

298 • Facilitate decision making when allocating budget, staffing, and other resources

299 • Communicate cybersecurity posture in a consistent way with community partners (e.g.,
300   vendors, supply chain, service providers), standards bodies, or regulators

301 **Assessing Current State**

302 Community Profiles can serve as valuable tools for assessing both the
303 community and organizations within the community. At the community
304 level, Profiles can help a community determine where its ecosystem has
305 systemic cybersecurity challenges and work in collaboration to address
306 those challenges.

307 In addition to using Community Profiles to create an Organizational
308 Target Profile, organizations can use the information in Community
309 Profiles to inform how they conduct internal assessments of their
310 progress in relation to community expectations. Communities may
311 choose to include assessment criteria and implementation examples to
312 facilitate consistent evaluation by community members. These
313 assessments will inform Organizational Profiles and strategic planning
314 efforts for organizations in the community.

315 For more information on Organizational Current Profiles and Target Profiles, see the *Creating*
316 *and Using Organizational Profiles Quick Start Guide*.

317 **3.4. Maintain**

318
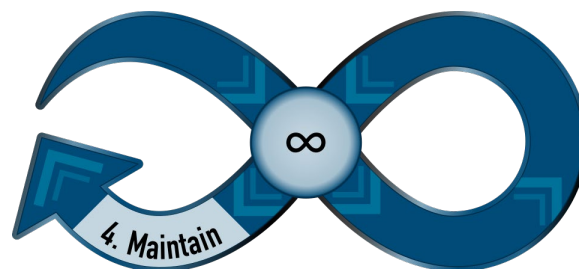
319 Collaboration across the community continues to maintain the Community Profile over time.
320 Perform the following activities:

321 • **Measure the impact the Community Profile is having and determine whether**
322   **additional resources are necessary to support successful use.** Communities may
323   conduct activities to measure the impact a Community Profile is having over time. Each
324   community will determine its need for measurement and effective measures for
325   evaluating impact. Understanding use and impact can also inform next steps for
326   maintaining the Community Profile and help the community identify any additional

327   resources it may need for effective use. For example, communities may choose to
328   develop guidance for implementation and assessment, establish a forum for ongoing
329   collaboration, or perform other activities.

330   • **Identify and monitor for changes and feedback that might necessitate updates.** As
331   operating environments and cybersecurity risks inevitably change over time, Community
332   Profiles will also need to change. Communities will need to determine an appropriate
333   frequency with which to review their Community Profiles, as well as any circumstances
334   that may necessitate change between periodic reviews. Examples of events that may
335   trigger the need to update a Community Profile include:

336   o   Changes to:

337   –   priorities

338   –   risk management posture (e.g., new threats)

339   –   laws, regulations, standards, contracts

340   –   sector composition

341   –   supply chain

342   –   insurance

343   o   Feedback from the community (e.g., clarity or utility of content, implementation
344   challenges)

345   o   Updates to the CSF

346   • **Update the Community Profile when needed by repeating earlier lifecycle phases.**
347   When changes are required, communities can follow earlier steps in the Community
348   Profile Lifecycle to make and communicate updates. Communities may also consider
349   whether and how to maintain an archive of previous versions of Community Profiles.

350   • **Retire Profiles.** Communities may also determine that a Community Profile has outlived
351   its usefulness and should be retired. Each community can determine its approach to
352   retiring Community Profiles.

353 **4. NCCoE Resources**

354 For more information regarding developing and using Community Profiles, see the NCCoE
355 Framework Resource Center and join our community of interest by sending an email to
356 framework-profiles@nist.gov.