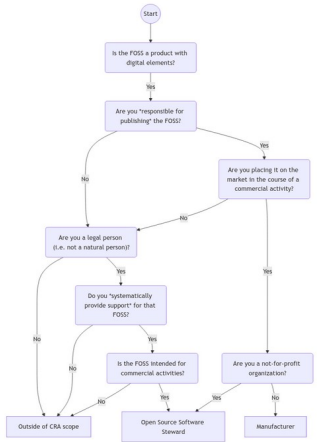
Organisation/individual	CPAN Security Group (CPANSec)
Date	2026-April-13
Other relevant info	About the contributors: CPANSec is the largest group of volunteers dedicated to improving the security of both the CPAN ecosystem, it's services and the Open Source Software components published there. CPANSec is also a CVE Numbering Authority for Perl and CPAN. CPAN (the Comprehensive Perl Archive Network) is the worlds oldest Open Source progamming language ecosystem, operating continuously since 1995. Salve J. Nilsen <sjn@cpansec.org> speaks on behalf of CPANSec. Additionally, we've received advice from Laurent Housen <lh@oaklaw.eu>, of OAK law firm in Brussels.

Organisation/individual	Item number	Comments	Proposed change
Salve J. Nilsen (CPANSec)	F.9	"Due diligence of third-party components" needs to include steps that relate to the long-term sustainability of the project, so that the Manufacturer can be sure the component's long-term security is taken care of.	
Salve J. Nilsen (CPANSec)	P.40	The CPAN (Comprehensive Perl Archive Network) is an example of an OSS publishing ecosystem, where there are no entities fall naturally under the "Steward" definition as it is presented here. The maintainers themselves are responsible for publishing on the platform, and the platform host organziation (itself a volunteer-run hobby project) is neither interested or capable of doing anything more than hosting the OSS. The CPAN is therefore a case where there is a need for a "Supporting entity" that assists OSS published on it's platform, but which isn't itself a publisher of said software.	
Salve J. Nilsen (CPANSec)	F.1	What if the Steward is not responsible for publishing, but still systematically provides support and makes sure that a give release of the FOSS is intended for commercial activities?	
Salve J. Nilsen (CPANSec)	F.1	The flowchart leaves out some common cases in the open source domain: 1) The publishing entity isn't a central organization, but rather the individual maintainer of a project, or a designated person (e.g. a co-maintainer); 2) The ecosystem services themselves are not a single project, but rather 3-4 independent projects that have a shared cooperation and understanding of roles, including retaining the ability for two of them be capable of replacing the third if it somehow is ompromised; 3) There are no natural central steward organizations that fit well with this model of operating, including the Perl Foundation (who isn't involved in any way in running the infrastructure); A change in this flowchart that can help make this possible, is to move the "systematically provide support" as the next question after answering "No" to the "Are you responsible for publishing the FOSS". The goal is to recognize that this community (or any other in a similar situation) may set up a separate support organization to fulfill the requirements coming from the CRA, but which may be community owned (e.g. creating a steward organization that operates as a maintainer-owned cooperative)	Please see https://github.com/orcwg/orcwg/issues/275#issuecomment-4162404856 for an example diagram. 

Salve J. Nilsen (CPANSec)	P.58	Can a Steward organization donate to the maintainer of an OSS project, proportionally based on the steward's sale of Voluntary Security Attestations? What happens if the donation amount becomes substantial enough to cover the Maintainer's expenses. Does the Steward (who can only donate to non-profits) have to stop donating? Some guiding examples would be helpful here.	
Salve J. Nilsen (CPANSec)	P.58	Can a Steward organization donate to the Maintainer, if the Maintainer is a co-owner of the Steward organization that supports it? (e.g. when the Steward is operated as a not-for-profit cooperative owned by Maintainers and other members of the ecosystem community/platform the Maintainer publish their software on). A clarifying example would help here.	
Salve J. Nilsen (CPANSec)	P.63	Since Stewards that operate as non-profits require any surplus or profit to be donated to not-for-project objectives – Does this include supporting the maintainers (in their personal capacity)? This is especially important in the transitional period when "hobby projects" will be looking to either find or create a Steward organization. Knowing that most OSS projects are maintained and published by natural persons, a Steward may still need to be able to "enroll" (or "convince") these projects with donations - even if it is not (yet) on a "sustained basis".	
Salve J. Nilsen (CPANSec)	P.63	Since the CPAN ecosystem/community has no suitable foundation or other organization that fits into the current idea of what is a "Steward", we are exploring the option to set up a dedicated organization specifically for this purpose. The best organizational structure for us, is to create a Non-profit Cooperative, as we wish that the entity supporting our ecosystem (and the 1000's of projects published there) should be Community and Maintainer-owned. We would like to see options like these to be made clear are acceptable. – Meaning – There should NOT be a base assumption that a "Steward" is a "Foundation", as this is the common interpretation.	
Laurent Housen (OAK law firm)	P.63	See comments from Salve J. Nilsen (CPANSec)	Where a legal person publishing a FOSS is a not-for-profit organisation ‘set up in such a way that ensures that all earnings after costs are used to achieve not-for-profit objectives’ (recital 18 of the CRA), the FOSS it publishes is not considered to be placed on the market. Where that legal person meets the definition of ‘steward’, it is subject to the corresponding obligations (Article 24 of the CRA). The legal person’s corporate set-up shall have no bearing on its qualification as a not-for-profit organisation provided that its internal rules, such as its articles of incorporation or other contractual commitments amongst its shareholders provide that all of its after costs earnings are allocated to not-for-profit objectives

Laurent Housen (OAK law firm)	E.18	To be sure that such explanations are clear, I also suggest adding the following example to follow example 18:	Example X: A legal person organised under non explicitly not-for-profit form such as a Cooperative or a Limited Liability Company with a social goal may also be considered a not-for-profit legal person under these Guidelines as long as its internal rules provide that the all its earnings after costs are used for not-for-profit objectives
Salve J. Nilsen (CPANSec)	P.72	Does "sustained support" include setting up and funding (e.g. through the sale of voluntary attestations) a regular and sustained donation regime for the FOSS projects under the Steward's care? Our assumption is yes, but an explicit example to confirm would be helpful.	
Salve J. Nilsen (CPANSec)	P.75	Foundations are not the only way of organizing sustained support. For example, a supporting entity (Steward) could be organized as a Maintainer-owned cooperative.	
Salve J. Nilsen (CPANSec)	P.75	Some clarity around the term "intended for commercial activities" would help here. For example, is it up to the component/OSS project's maintainer to decide if their project is "intended for commercial activities"? Or is it implied that an OSS is such, if the project has a Steward, and publishes the necessary documentation and metadata required to successfully take part in the security regime implied in the CRA?	
Salve J. Nilsen (CPANSec)	P.79	Please add an example, where the Steward may inform their users about a vulnerability by publishing or issuing a CVE for said vulnerability. As it stands now, the text is a bit confusing.	
Salve J. Nilsen (CPANSec)	P.84	Additional example wanted: When a Non-profit cooperative supports projects published through an ecosystem (package publishing platform), and where the projects are intended for commercial use, and where any sales of voluntary attestations are used to offer sustained support to not just the projects in question, but also related communities and services, and relevant/affected upstream or downsteam projects and comminities.	
Salve J. Nilsen (CPANSec)	P.84	Additional example wanted (variation of E.28): Same as Example 28, but the project chooses or comes to agreement with their ecosystem steward, by joining their cooperative in order to get support from it, and take part in the voluntary attestation regime they are managing.	
Salve J. Nilsen (CPANSec)	P.155	Due diligence should not only verify if components satify any specific requirements, but also include taking any action at correcting any required incomplete, misleading or wrong information	