Nemko Digital

Mastering CRA - Cyber Resilience Act Practical Steps for Trustworthy Systems

---

1
00:00:06.480 --> 00:00:18.499
Bas Overtoom: Hello, everybody, and welcome to this webinar on mastering the Cyber Resilience Act. My name is Bas Overtoom, and I'm happy that you're here to join us.

2
00:00:18.500 --> 00:00:29.159
Bas Overtoom: to look at these very interesting regulations and everything that is to do for it, for your products and your organization. I'm here with two gentlemen, and they will introduce themselves in a minute.

3
00:00:29.270 --> 00:00:36.909
Bas Overtoom: And we're happy to help you going and get through this, let's say, important steps that you need to start taking.

4
00:00:37.790 --> 00:00:56.570
Bas Overtoom: So, this is a bit of the agenda of today. I'll give a very short introduction of a couple of minutes on our organization, then the initial focus of the part is really on the Cyber Resilience Act as such, the timeline, the scope, the requirements, and what is a good approach

5
00:00:56.570 --> 00:01:21.520
Bas Overtoom: towards compliance, and then in the second part, we will focus a bit more on, yeah, getting ready for the testing, and in the end, the validation and certification process that is also required for, at least for some of the products that fall

under the CIA. So that's basically the part, and then we'll end with some conclusions on, yeah, really how to get started and boiling it all down to making

6
00:01:21.520 --> 00:01:40.700
Bas Overtoom: it very concrete for you. We hope to do this in about 30 minutes, and then we have, for step five, another 15 minutes for Q&A. So, yeah, later on you can, if you have any questions, you can type them away in the chat, and we'll try to answer as much as possible.

7
00:01:40.700 --> 00:01:46.339
Bas Overtoom: During the 15 minutes that we have, and else we will get back to you via an email.

8
00:01:46.340 --> 00:02:11.300
Bas Overtoom: So, great, you can also be here. We had lots and lots and lots of, people registering, and now also, yeah, more than 200, almost 300 people in the call, so I can honestly say that this is a very, very hot topic in the market. So, great that you can all join. So, I already introduced myself, maybe the two gentlemen that are going to do this webinar with me, Daniel.

9
00:02:11.300 --> 00:02:14.379
Bas Overtoom: start with you. Maybe you can say a few words about yourself.

10
00:02:15.380 --> 00:02:24.390
Daniel Havre: Thank you, Baz. So my name is Daniel. I'm working as a cybersecurity evaluator here at Nemko.

11
00:02:24.390 --> 00:02:36.440
Daniel Havre: Has been doing so for a little over 5 years, doing a range of different security evaluations according to different regulations and directives.

12
00:02:36.560 --> 00:02:50.120
Daniel Havre: preparing for the CRA these days, but also do common criteria evaluations, security evaluations according to the Radio Equipment Directive, and, yeah, as I mentioned, a couple of others.

13
00:02:51.050 --> 00:02:55.669
Bas Overtoom: Great. Thank you for joining and sharing your knowledge. Papain.

14
00:02:56.640 --> 00:03:20.590
Pepijn van der Laan: Yes, so I'm Pep, I'm the technical director at, at Nemko Digital, so yeah, I see in the bio it says over 10 years, well, yeah. Okay, that's to make me, look young, I think. So I have, extensive experience in, AI data, delivering digital, digital products, so, of course, that also includes a strong, strong security,

15
00:03:20.740 --> 00:03:30.260
Pepijn van der Laan: component, which is getting ever more important, so great to be here with you today to talk about, in particular, the Cyber Resilience Act.

16
00:03:30.880 --> 00:03:32.919
Bas Overtoom: Okay, now, without the…

17
00:03:33.610 --> 00:03:55.699
Bas Overtoom: do any more time, let's dive into it. Nemko, Nemko, 90 years of history, of course, many of you know about it. The digital arm that Papain and myself are leading, we set up two years ago in 2024, and we really focus on the digital part. So that is, of course, AI data, but of course, also

18
00:03:55.700 --> 00:03:58.470
Bas Overtoom: Cyber is an important part of that.

19
00:03:58.510 --> 00:04:23.139
Bas Overtoom: And, yeah, we do that also together with our colleagues from the Nemko group, which are more responsible for, let's say, the testing part, and we, as Nemko Digital, are focused a bit more on the consulting and the advisory part. And with that, you will also see in this presentation that we really offer this end-to-end service and support to kind of comply with CRA. Yeah, we will talk about it, we'll show also different client cases in this webinar to make it very tangible.

20
00:04:23.450 --> 00:04:36.839
Bas Overtoom: for you. These are some of the services that we deliver. On the left-hand side, it is basically all about product compliancy, so regulatory compliance, like an EOAI Act, like the CRA, like a data act, these kind of things.

21
00:04:36.840 --> 00:04:51.620
Bas Overtoom: ISO certifications for your organization, global market access, because it's not only in Europe that you need to comply, but it's all around the world, so we do global market regulatory monitoring, we do global market access projects, we have our own Trustmark.

22
00:04:51.620 --> 00:05:07.900
Bas Overtoom: And on the right-hand side, you see a bit more, let's say, on the kind of the organizational advisory support that we're offering, that is, on the one hand, setting up processes, but also helping to implement monitoring tools for, for example, for AI, but it can also be for cyber or

23
00:05:07.900 --> 00:05:31.290
Bas Overtoom: data management. So, this is, let's say, our broad package that we are servicing, but today it's all about cybersecurity, and it's all about CRA. So, I think enough on the introductions. Let's dive into it. The first part, I give the word to Papain, maybe to bring us along. What is this CRA, and how are we looking into that, specifically in the client cases.

24
00:05:31.290 --> 00:05:34.059
Bas Overtoom: for similar companies as yourself. Bye-bye.

25
00:05:34.950 --> 00:05:39.819
Pepijn van der Laan: Yeah, thanks, thanks, boss. Thanks for the introduction. So,

26
00:05:39.850 --> 00:06:02.030
Pepijn van der Laan: CRA, of course, part of a much broader, digital regulations framework within the European Union. As you can see on this slide, yeah, there's a lot of deadlines, coming after, coming after us these days, yeah? A lot of, different, different boards on which you have to play, play chess and make sure that you're in the best,

27
00:06:02.030 --> 00:06:04.780
Pepijn van der Laan: Positioned towards compliance.

28
00:06:05.700 --> 00:06:18.629
Pepijn van der Laan: So, for the Cyber Resilience Act, two dates, one in September 2026, one in December 2027, that are, that are key dates when it comes to, when it comes to compliance.

29
00:06:18.650 --> 00:06:36.199
Pepijn van der Laan: So definitely, for many people in the compliance field, not the only thing to worry about, but it is an important one, and also one that deserves separate attention, hence this webinar. But let's dive a little bit further into the CRA itself on the next slide.

30
00:06:38.000 --> 00:06:39.040
Pepijn van der Laan: So…

31

00:06:39.110 --> 00:06:58.110
Pepijn van der Laan: what it is about, it's really about reducing the cybersecurity vulnerabilities for product with digital elements, so that brings us to the first key concept of the CRA. So this means it is concerned both with hardware and software elements of your product.

32
00:06:58.110 --> 00:07:17.510
Pepijn van der Laan: It includes also remote data processing, apps, so processing at a distance, which is, of course, also, yeah, indispensable for many of our app products these days. And it's not only the product as it goes to market, it's also really

33
00:07:17.510 --> 00:07:27.760
Pepijn van der Laan: a support period, so basically across that whole life cycle of the product, you'll have the obligations of the Cyber Resilience Act. And

34
00:07:28.030 --> 00:07:47.699
Pepijn van der Laan: not just for the things that you're doing on that yourself, but there's also a supply chain element to it. The software bill of materials is a super important concept here, to understand what are the different vulnerabilities that come from the different elements of which your product is composed.

35
00:07:47.840 --> 00:07:48.720
Pepijn van der Laan: So…

36
00:07:49.160 --> 00:08:07.689
Pepijn van der Laan: key dates, I already mentioned them briefly, so September this year, so only a few months, away, the mandatory, incident, report, or reporting for, for manufacturers who must be able to, to report serious, serious incidents, and, within strict timelines.

37
00:08:07.690 --> 00:08:13.569

Pepijn van der Laan: And then towards the end of 2027, the full compliance with the CRA.

38
00:08:13.570 --> 00:08:17.719
Pepijn van der Laan: Where non-compliant products can also not be sold anymore in the…

39
00:08:17.750 --> 00:08:33.909
Pepijn van der Laan: in the EU. So, quite some, has some timelines there that you need to be aware of. Before diving further in the CRA, briefly, a little digression to some of the related regulations that make

40
00:08:34.159 --> 00:08:41.190
Pepijn van der Laan: compliance with the CRA, even more, important, so on the next, on the next slide.

41
00:08:41.190 --> 00:08:59.300
Pepijn van der Laan: you'll see some of the, some of the connections there. So, first one to mention here is, of course, the… the radio equipment, directive, which, which covers more the physical side of, of the devices with, with radio,

42
00:08:59.300 --> 00:09:11.219
Pepijn van der Laan: equipment, so that, the CRA really leverages some of the, of the elements of that, of that RED directive. So, RED compliance brings you.

43
00:09:11.270 --> 00:09:12.630
Pepijn van der Laan: towards…

44
00:09:12.790 --> 00:09:26.410

Pepijn van der Laan: CRA compliant, but not there. There is… there's more from a CRA perspective that you need to do, so if you are RED compliant, you are not yet there, that's important to realize. Additional effort is needed.

45
00:09:26.920 --> 00:09:33.680
Pepijn van der Laan: Another cross-connection in that, in the digital, in the digital framework is with the AI Act.

46
00:09:33.680 --> 00:09:56.059
Pepijn van der Laan: So when it comes to artificial intelligence, there's an important connection. If you have high-risk AI systems, and for those who can prove that they comply with the CRA requirements, then that gives you also the presumption of conformity for the cybersecurity requirements that are part of the AI Act.

47
00:09:56.060 --> 00:10:10.299
Pepijn van der Laan: So also, from that aspect, following the CRA requirements is an important, is an important step, and also a step that will help you towards, towards AI Act compliance for high-risk systems.

48
00:10:11.320 --> 00:10:30.859
Pepijn van der Laan: And of course, there are also, exceptions for specific, product categories, so some examples mentioned there, so let me not go into those in, in detail. But let's instead look at the different categories of, of products, which you have on the next,

49
00:10:31.090 --> 00:10:33.050
Pepijn van der Laan: Which we have on the next slide.

50
00:10:33.230 --> 00:10:34.659
Pepijn van der Laan: So…

51
00:10:34.850 --> 00:10:48.489
Pepijn van der Laan: basically has… what you see here, as you see it in more of those recommendations, is basically the classification in different types of products, which, in the case of CRA, lead to

52
00:10:48.600 --> 00:11:06.320
Pepijn van der Laan: different requirements in terms of horizontal versus vertical standards, but also lead to stronger requirements when it comes to proving the conformity. For the default product, you can do self-declaration,

53
00:11:06.550 --> 00:11:23.600
Pepijn van der Laan: But when you get into important products, critical products, it really is a conformity assessment by a notified body, and in some cases, even a cybersecurity certificate that is required, if that's applicable to the product category.

54
00:11:23.600 --> 00:11:30.569
Pepijn van der Laan: So, there you see, that it's already important to understand that which, at which,

55
00:11:31.160 --> 00:11:33.130
Pepijn van der Laan: Scheme you fall under.

56
00:11:34.980 --> 00:11:44.369
Pepijn van der Laan: And then, kind of, from there, looking a little bit at the high levels already on the, on the requirements on the next, on the next page.

57
00:11:46.170 --> 00:12:03.979
Pepijn van der Laan: So, important to realize that what you see, and that is something that you see increasingly in those, in those EU regulations, is that it's not just about the product, it's also about the process, right? It is,

58
00:12:03.980 --> 00:12:19.780
Pepijn van der Laan: In particular, with digital regulations, you see that, yes, there are the product requirements about security by design, by default, data minimization, resilience, what have you, but there's also the process behind it.

59
00:12:19.780 --> 00:12:39.459
Pepijn van der Laan: In terms of the risk assessment, the risk management, the testing and review, the documentation that you need to have in place, and the continued dissemination of security updates. So both on the product side, as on the process side, there are quite some requirements. So, if you give this one more click.

60
00:12:42.390 --> 00:12:44.449
Pepijn van der Laan: Then you see,

61
00:12:44.820 --> 00:12:55.659
Pepijn van der Laan: that this also requires quite something from organizations. It's about integrating the product security and the organizational governance.

62
00:12:55.660 --> 00:13:06.150
Pepijn van der Laan: So you have to really reach beyond silos there. It's about moving from ad hoc controls to really something that is also captured in a process.

63
00:13:06.150 --> 00:13:13.760
Pepijn van der Laan: embedding also the continuous, nature of vulnerability management. So there's…

64
00:13:13.760 --> 00:13:29.469

Pepijn van der Laan: quite something there when you look at it, what this means if you want to make your organization ready for it. In particular, if you have a broader range of products and maybe multiple divisions that are part of the scheme.

65
00:13:29.610 --> 00:13:44.439
Pepijn van der Laan: So, managing that complexity is also something where we see, our clients, sometimes, running into, into challenges. Some common challenges, which we can, can mention on the, on the next slide.

66
00:13:45.780 --> 00:13:58.590
Pepijn van der Laan: So, first of all, there is, has something that, yeah, it's basically, the unclarity about standards. So, a lot of the standards are still in draft, horizontal standards, vertical standards.

67
00:13:58.590 --> 00:14:17.750
Pepijn van der Laan: So there is quite, yeah, quite a need for, yeah, for stepping, yeah, for basically creating the clarity and creating the, the definition of done there. Yeah, where can you already, count on, but also what are the, the things that are maybe still, still uncertain?

68
00:14:18.010 --> 00:14:26.009
Pepijn van der Laan: You run into decentralized processes, which is something that, if you want to bridge that gap between the product and the process level.

69
00:14:26.340 --> 00:14:41.880
Pepijn van der Laan: is something that can lead to additional complexity that you need to manage. A lot of independently operating product teams with fragmented ownership across departments is something we see often.

70
00:14:42.120 --> 00:14:57.239

Pepijn van der Laan: limited visibility on software components. In particular, there's also a lot of, external suppliers, in there, resource and capability constraints, organizational readiness,

71
00:14:57.460 --> 00:15:11.479
Pepijn van der Laan: also something that we typically see there. So, let me, let me move on, show a little… yes, show what we… what we also on the… yeah, on the, on the draft standards. Yes, thanks, boss,

72
00:15:12.040 --> 00:15:22.670
Pepijn van der Laan: There are quite some, yeah, some standards in the making, yeah, quite some in, yeah, in public inquiry and preview, some still being drafted.

73
00:15:23.020 --> 00:15:44.470
Pepijn van der Laan: couple published, so this is a, yeah, constantly shifting landscape, of course, that we also closely, closely monitor in order to make sure that we can also advise our clients in the best possible way on where to basically count on the standards, but also where, we should go, really, for the…

74
00:15:44.470 --> 00:15:48.680
Pepijn van der Laan: for the text of the CRA itself when it comes to proving the conformity.

75
00:15:50.490 --> 00:15:51.470
Pepijn van der Laan: So…

76
00:15:51.810 --> 00:16:11.030
Pepijn van der Laan: how we typically approach that journey towards conformity is what we show here. It's a phased approach, which starts in particular for larger organizations, often with a piece of discovery and alignment, where we get the clarity on

77
00:16:11.520 --> 00:16:19.890
Pepijn van der Laan: what are the challenges, ahead, what are the, the elements that are, that are, that are under the CRA scope?

78
00:16:19.890 --> 00:16:34.979
Pepijn van der Laan: but also agree on the principles, the roles, the decision-making on the organization side. And from there, of course, looking closer at the applicability, the specific requirements, what are the gaps in the roadmap to…

79
00:16:34.980 --> 00:16:37.869
Pepijn van der Laan: To basically remediate those,

80
00:16:38.150 --> 00:16:54.400
Pepijn van der Laan: providing the support and remediation and, and controls, towards, in the end. Had the validation testing certification, which then runs into, of course, execution and monitoring on an ongoing basis.

81
00:16:55.610 --> 00:17:00.179
Pepijn van der Laan: To make this concrete in the case example.

82
00:17:00.180 --> 00:17:16.960
Pepijn van der Laan: So this is a case example of an IoT company, where we focused ourselves really on a specific line of product, so they're stepping into that second, part of, second step of the, of the journey, really.

83
00:17:16.960 --> 00:17:34.410
Pepijn van der Laan: Helping them to reprioritize internal projects based on the applicability matrix that we constructed to really understand those regulatory obligations and identify the gaps towards compliance.

84
00:17:34.410 --> 00:17:40.199
Pepijn van der Laan: So that really helps in terms of accelerating the road to compliance, where we also

85
00:17:40.200 --> 00:17:51.000
Pepijn van der Laan: have from Nemko can support, hands-on with, for example, the soft controls, which then, in this case, really freed up the technical resources at the client.

86
00:17:51.000 --> 00:17:52.250
Bas Overtoom: to.

87
00:17:52.640 --> 00:17:57.770
Pepijn van der Laan: To really, focus on what they're, basically indispensable for.

88
00:17:58.760 --> 00:17:59.680
Pepijn van der Laan: So…

89
00:18:00.560 --> 00:18:12.019
Pepijn van der Laan: how did we… how did we do that? On the next slide, briefly, the process, there you see the same type of steps, part of that journey that I showed… showed before.

90
00:18:12.310 --> 00:18:28.929
Pepijn van der Laan: Starting from the applicability towards the gaps, and from there, remediation support, which we can do in a very flexible way, and at the same time, also, the regulatory radar, which helps us to basically,

91
00:18:28.930 --> 00:18:40.919

Pepijn van der Laan: Basically, create for our clients the clarity of, yeah, where are things changing? What are the new developments that you need to anticipate on when it comes to the development of standards.

92
00:18:42.590 --> 00:18:49.459
Pepijn van der Laan: So… In the end, that leads then to, indeed, a list of,

93
00:18:49.520 --> 00:19:12.550
Pepijn van der Laan: yeah, of deliverables that we need to, to deliver in order to get, and this is, of course, a high level, that we need to, deliver in order to get towards compliance, where we also, together with the client, decided, okay, what are the things that we can execute on as, as Nemko, where we can really kind of do the heavy lifting, and what are the parts that are more,

94
00:19:12.800 --> 00:19:13.550
Pepijn van der Laan: The…

95
00:19:13.700 --> 00:19:22.990
Pepijn van der Laan: The place for us to consult, where it is the client's, the client's own team that's really driving the… driving the change and driving the media for us.

96
00:19:23.370 --> 00:19:29.940
Pepijn van der Laan: But that gives you a little bit of a flavor of the CRA, as well as how we support our clients on that.

97
00:19:31.430 --> 00:19:40.529
Bas Overtoom: Thank you, Papain, very insightful, and I think before we make it even more concrete with the story of Daniel, maybe it's good to get a little bit of your,

98
00:19:40.550 --> 00:19:59.589

Bas Overtoom: the temperature where you are standing, so it's time for the poll, right now. You will see it coming up in a minute, and then the question we have to you is, yeah, where are you when it comes now to the, to the CRA? Are you on the page, like, teach me everything?

99
00:19:59.590 --> 00:20:15.179
Bas Overtoom: Or, yeah, we need really structure and support. I think we've got this, it's just more of a sanity check that we're in. We're almost there. This is just a final validation, or, yeah, we feel we have managed this, just to get a little bit of an understanding where you are. So the poll is coming up.

100
00:20:15.200 --> 00:20:35.130
Bas Overtoom: Right now, take your time to kind of fill in your vote, and in the end, with the Q&A, we'll also share a little bit of the insights, where this audience is, and since we are with over 300 people, I think it is also giving, let's say, a good understanding of where you are in the market, and I'm curious to see the results, so…

101
00:20:35.130 --> 00:20:41.690
Bas Overtoom: While you're filling in your, your thing, we are moving ahead to the kind of the second part of the, of the introduction.

102
00:20:41.800 --> 00:20:58.799
Bas Overtoom: And, yeah, Daniel, I'm gonna give the word to you. Get ready for testing. So, you're, of course, the CRA testing expert, a little bit further in the journey than Papain, who was more, let's say, early in the journey, getting people ready for testing and validation, but at one point, yeah, we come to you, so…

103
00:20:58.860 --> 00:21:03.970
Bas Overtoom: Tell us what you are looking for and the approach to get ready for testing.

104

00:21:04.880 --> 00:21:17.350
Daniel Havre: Yes, thank you, yeah. So, how to prepare, prepare for the Cyber Resilience Act? The overall goal, as Pepe has said, is that, it's to ensure that digital

105
00:21:17.400 --> 00:21:32.040
Daniel Havre: connected hardware and software products placed on the EU market are more secure. Also, as mentioned, there are some new terms compared to those few who have already been doing,

106
00:21:32.040 --> 00:21:50.399
Daniel Havre: the radio equipment directive, and perhaps some industrial cybersecurity assessments, and those terms are secure by design, and secure by default. So, the secure by default means that it should be secure basically out of the box, and when it's set up.

107
00:21:50.840 --> 00:22:09.930
Daniel Havre: And secure by design means that there will be some, some, specific requirements, during the, design phase of the equipment, like, which, yeah, like secure coding and, and, and, and such things.

108
00:22:10.320 --> 00:22:23.619
Daniel Havre: The risk analysis that's needing to be done is on the intended purpose and reasonable foreseeable use for the, which is specific for the cyber resilience sectors.

109
00:22:24.490 --> 00:22:34.889
Daniel Havre: And also, the manufacturers will remain responsible for the product's cybersecurity for a minimum of 5 years after sales.

110
00:22:34.890 --> 00:22:45.039

Daniel Havre: So, combine this with the secure by design requirement and the product-specific requirement, which I will briefly touch upon

111
00:22:45.210 --> 00:22:52.009
Daniel Havre: Then you have the, basically the entire lifecycle of the, product.

112
00:22:52.660 --> 00:23:01.040
Daniel Havre: And, also, as Papen said, the reporting of exploitable security vulnerabilities of product is a,

113
00:23:01.560 --> 00:23:06.670
Daniel Havre: A requirement, together with the risk classification and classes.

114
00:23:07.180 --> 00:23:09.069
Daniel Havre: So, next slide. We…

115
00:23:12.470 --> 00:23:28.169
Daniel Havre: Yeah, so we see that the harmonized standard is not required to get going. The default category does not need… does not require to use harmonized standards. The requirements, the essential requirements, are listed in the Cyber Resilience Act itself.

116
00:23:28.540 --> 00:23:38.450
Daniel Havre: In Annex 1, Path 1, we have the central cybersecurity requirements, or the product requirements, as I like to call them.

117
00:23:38.610 --> 00:23:49.789
Daniel Havre: These are the requirements that is specific for the equipment, software, hardware, in questions that need to be, CE marked.

118
00:23:49.920 --> 00:24:00.760
Daniel Havre: And the part two, which is another important thing, is the vulnerability handling requirements, or the procedural requirements on how you address incoming.

119
00:24:00.960 --> 00:24:04.050
Bas Overtoom: Reports of.

120
00:24:05.590 --> 00:24:21.349
Daniel Havre: of vulnerabilities and exploits, as well as how you monitor and ensure the software bill of material is updated and secure. And lastly, there is in Annex 1 some information and instructions to the user.

121
00:24:22.070 --> 00:24:28.760
Daniel Havre: Yeah, so it's, your typical CE marking directive.

122
00:24:29.220 --> 00:24:38.780
Daniel Havre: If we go to the next slide, we can see the overview of the essential requirements that are for the product-specific ones.

123
00:24:38.990 --> 00:24:52.709
Daniel Havre: You have the risk assessment, the secure design, development, and production. You also have the no-known exploitable vulnerabilities, the secure by default configuration, which is a new, or relatively new.

124
00:24:53.070 --> 00:25:05.409
Daniel Havre: requirement, depending on… on what you have previously been… been doing. Looking at the other requirements, the security updates is,

125
00:25:05.560 --> 00:25:16.299

Daniel Havre: A requirement that's present in many other standards, also some access control and authentication requirements, integrity and confidentiality.

126
00:25:16.530 --> 00:25:23.329
Daniel Havre: is also, elements that we see in many other standards. So,

127
00:25:24.370 --> 00:25:38.239
Daniel Havre: Yeah, I won't go through all of them due to the time, but this gives you an overview of what is it your products will need to satisfy in terms of what mechanisms or…

128
00:25:38.400 --> 00:25:43.309
Daniel Havre: Overview of, the security that needs to be, in place.

129
00:25:44.910 --> 00:25:50.430
Daniel Havre: Moving on to the next slide, we have the essential requirements for the vulnerability handling.

130
00:25:50.660 --> 00:25:52.819
Daniel Havre: Which is listed in Annex 1.

131
00:25:53.640 --> 00:26:11.340
Daniel Havre: And here you have your, identify and document the vulnerabilities and components, including maintaining the software bill of material, which means that you need to have an overview of all the software that is in your equipment.

132
00:26:12.820 --> 00:26:30.039
Daniel Havre: There is also requirements regarding providing updates and needing to do tests, regular tests and reviews of the security, because you need to keep your product secure for a minimum of 5 years.

133
00:26:32.170 --> 00:26:36.670
Daniel Havre: Moving on… If we can go to the next slide…

134
00:26:37.010 --> 00:26:50.140
Daniel Havre: This is also the information provided with the product. I think I will just show it there, and since we are delivering the PowerPoint afterwards, you can take a closer look at it, so we can…

135
00:26:50.340 --> 00:26:51.989
Daniel Havre: Jump to next slide.

136
00:26:54.410 --> 00:27:01.550
Daniel Havre: So, a typical cybersecurity evaluation process contains mainly of two main steps.

137
00:27:01.720 --> 00:27:15.349
Daniel Havre: It's the step one, it's the documentation, and step two is the functional testing or verification, all dependent on what type of product you have, or what type of standard you are…

138
00:27:16.610 --> 00:27:28.420
Daniel Havre: lying for. So the documentation includes, the documentation of the security development vulnerability handling. It will also include the product context and product security.

139
00:27:28.590 --> 00:27:44.040
Daniel Havre: The product context, there is a standard currently being developed by the EN. It's the 40,000-1-2, which is the product context standard, currently in draft mode, as of today.

140
00:27:44.250 --> 00:27:53.759
Daniel Havre: And the product security will also be addressed by the EN4000-1-4, which is, currently being developed.

141
00:27:54.490 --> 00:28:04.400
Daniel Havre: And this is hopefully, or it's, will maybe be the, horizontal standard in the future.

142
00:28:05.910 --> 00:28:15.450
Daniel Havre: If not, there is a range of vertical standards that are currently being developed for the product-specific requirements for the Cyber Resilience Act.

143
00:28:16.640 --> 00:28:34.099
Daniel Havre: And step two is the functional testing and verification, which, depending on what type of product and product category you are in, the amount of testing will differ between the standard, or that's at least what we see from

144
00:28:34.370 --> 00:28:41.649
Daniel Havre: from, the standards today. And the output, or step 3, is a report

145
00:28:42.130 --> 00:28:46.719
Daniel Havre: Containing the information that,

146
00:28:46.960 --> 00:28:49.140
Daniel Havre: You get from Step 1 and 3.

147
00:28:49.320 --> 00:29:05.549

Daniel Havre: And as a warning, I usually say don't underestimate the documentation requirements. These are information that you need to document, and can, in some situations, be more than you think.

148
00:29:06.960 --> 00:29:11.150
Daniel Havre: If we go to the next slide, we can see a typical testing…

149
00:29:11.340 --> 00:29:21.440
Daniel Havre: scenario. So, for example, if you want to test a secure communication mechanism, you may or may not use a sniffing tool to monitoring the threat net.

150
00:29:21.550 --> 00:29:23.499
Daniel Havre: the, network traffic.

151
00:29:23.640 --> 00:29:36.330
Daniel Havre: So in this case, we have a Wireshark picture, which can be used to verify that the correct protocol is used. In this case.

152
00:29:36.430 --> 00:29:43.600
Daniel Havre: It's a, TSP TLS 1.2 protocol that is used, which…

153
00:29:43.930 --> 00:29:49.809
Daniel Havre: There are several TLS, protocols out there, and

154
00:29:49.960 --> 00:30:01.419
Daniel Havre: Each of these protocols use different cipher suites, and this is one way of verifying, or to check if

155
00:30:02.610 --> 00:30:05.940

Daniel Havre: If the documentation is correct,

156
00:30:06.660 --> 00:30:10.969
Daniel Havre: Based on what you have stated in the information.

157
00:30:11.240 --> 00:30:16.400
Daniel Havre: Moving on, we have the next typical testing case,

158
00:30:17.820 --> 00:30:31.990
Daniel Havre: is more of a passive scan. Typically, you can use a NMAP scan to verify what ports and services are open, to verify if there are any vulnerabilities, or…

159
00:30:32.320 --> 00:30:42.080
Daniel Havre: Attack services that are undocumented or are using unsecure, services, to, to,

160
00:30:42.210 --> 00:30:46.980
Daniel Havre: Communicate or operate, for the equipment.

161
00:30:47.210 --> 00:30:54.590
Daniel Havre: And I, posted in the bottom here, note the command is only used as a reference only, so…

162
00:30:55.780 --> 00:31:03.690
Daniel Havre: when Nemko does these types of scan, we will have a more accurate and more, including,

163
00:31:04.090 --> 00:31:07.450
Daniel Havre: scan, verifying not only the TCP ports, but…

164
00:31:08.490 --> 00:31:15.379
Daniel Havre: a lot of others. So these are just to, to, to briefly show you the, different types of,

165
00:31:15.570 --> 00:31:28.159
Daniel Havre: Test, which may or may not be applicable, depending on your product and what the test, or what the standal… what kind of test the standouts will…

166
00:31:28.410 --> 00:31:30.110
Daniel Havre: Require of you.

167
00:31:31.140 --> 00:31:32.189
Daniel Havre: So, thank you.

168
00:31:32.940 --> 00:31:39.850
Bas Overtoom: Alright, thank you very much, Daniel, for showing some light and giving some concrete examples, and of course, as

169
00:31:39.850 --> 00:32:04.390
Bas Overtoom: you mentioned already yourself, yeah, this is just an illustration to give a little bit meat on the bones of what to expect. Going back to the journey that the Papen mentioned earlier, so we're looking at testing, but testing is not step one, and I think, yeah, the amount of interest is there also today, when we feel that most people are getting started on CRA and the journey, and also from the

170
00:32:04.390 --> 00:32:21.960
Bas Overtoom: client conversations that we're having. So bringing it a little bit back to Papain, how do you get started now? Based on all this information that we can, that we

shared in 30 minutes, I think it can be a bit overwhelming, so please bring us back and try to make it concrete in, let's say, step one, because getting started…

171
00:32:22.020 --> 00:32:32.070
Bas Overtoom: is maybe just the most important step. So you cannot oversee everything, but just getting started as soon as possible is basically the key call to action we want to give to you. Bye-bye.

172
00:32:32.470 --> 00:32:55.670
Pepijn van der Laan: Yeah, exactly. In particular, considering the implications that, the dismay has, it's important to start and start thinking there already, yeah, in those two, in those two lanes that you see, yeah? On the one hand, it's about getting to compliance at the product level, it's on the other hand also about embedding this in your, in your organization.

173
00:32:55.670 --> 00:32:59.429
Pepijn van der Laan: So, what we often recommend there as a first step

174
00:32:59.430 --> 00:33:08.579
Pepijn van der Laan: is, to do that in, in a workshop, type, type setting. So, example, on the next, on the next slide.

175
00:33:10.160 --> 00:33:25.180
Pepijn van der Laan: Where we typically do discovery and alignment workshops with the key stakeholders to really make sure that we get all the involved stakeholders really on the same page.

176
00:33:25.180 --> 00:33:39.949
Pepijn van der Laan: When it comes to understanding the requirements and the impact also on their part of the business, but also the first clarity on, kind of, where are the gaps

in the processes, in the governance, but also what is then the strategic approach that we take.

177
00:33:39.990 --> 00:33:54.320
Pepijn van der Laan: towards that, CRA compliance? Is it every department for themselves? Do we really share processes and best practices? How are we going to collaborate? How are we going to make decisions?

178
00:33:54.320 --> 00:34:03.300
Pepijn van der Laan: Very important to make sure that you basically set that out in a clear way, because that is going to help you a lot.

179
00:34:03.860 --> 00:34:23.089
Pepijn van der Laan: in order to get successful, yeah, and typically in a domain like this, which is typically, yeah, when it comes to compliance, really very much a product domain as well, now really also reaching into the processes, into the organization side as well. So, laying the good groundwork, super important there.

180
00:34:23.090 --> 00:34:40.879
Bas Overtoom: Maybe to add to that, I think this is also mainly a step behind we see for the more larger multinational global companies to take. If you are a little bit of a, let's say, a small or medium-sized player, then maybe such a discovery alignment workshop is less needed than you.

181
00:34:40.889 --> 00:34:41.489
Pepijn van der Laan: Yeah.

182
00:34:41.489 --> 00:34:42.209
Bas Overtoom: Next step.

183

00:34:42.210 --> 00:34:56.149
Pepijn van der Laan: Yeah, so that's a nice bridge, boss, actually, to the next, to the next slide, because that also gives you the… if you only have a limited product range, yeah, then you can step directly into…

184
00:34:56.150 --> 00:35:04.599
Pepijn van der Laan: The next stage in the funnel, which is really getting the clarity on the applicability and the requirements.

185
00:35:04.670 --> 00:35:22.989
Pepijn van der Laan: Diving deep onto, okay, what is then the definition of done that we need to achieve? And what are then, based on what we have currently in place, in terms of information, in terms of processes, in terms of security measures in the product, what are then the gaps that we see?

186
00:35:22.990 --> 00:35:37.279
Pepijn van der Laan: And then you can start planning towards the remediation and towards the, in the end, the validation and the testing, the certification. So then you can take one step further into that… into that funnel. So that is really where it's more…

187
00:35:37.280 --> 00:35:43.730
Pepijn van der Laan: Assessment-type, type work, which is, which then really helps you to,

188
00:35:44.380 --> 00:35:52.019
Pepijn van der Laan: to create that definition of DOM. I believe that we have still one detailed slide, behind this.

189
00:35:52.020 --> 00:36:06.350
Bas Overtoom: maybe one point to make here, I think it is good to make the awareness that as Nemko, Digital and Nemko group combined, we can really bring you, support

you all the way to this journey, from the beginning to the, to the end, where, where required.

190
00:36:08.550 --> 00:36:10.509
Pepijn van der Laan: Yeah, thanks, thanks, boss.

191
00:36:11.840 --> 00:36:16.499
Pepijn van der Laan: So, and when it comes to this, to this part of the journey.

192
00:36:16.620 --> 00:36:35.150
Pepijn van der Laan: of course, applicability requirements, yeah, what we call an applicability matrix, to make sure that we get all those, those requirements and all those obligations really mapped out in such a way that it becomes, really your shopping list towards the, towards the definition of DOM.

193
00:36:35.500 --> 00:36:45.030
Pepijn van der Laan: From there, then comparing that to, okay, yeah, what is then the current state, which is something that we can, often do.

194
00:36:45.030 --> 00:36:55.599
Pepijn van der Laan: Much more pragmatically than really, kind of, doing the end-to-end testing, so that we really have a number of interviews with the relevant people, that we basically map out the

195
00:36:55.600 --> 00:37:12.400
Pepijn van der Laan: basically had the gaps and the risks towards, towards compliance, and really then helping translate that into a concrete roadmap with, which helps you to set the priorities and, and basically plan out in time,

196
00:37:12.640 --> 00:37:21.620

Pepijn van der Laan: With, with clear milestones and also responsibilities internally, so that it becomes something that is then manageable towards the… towards the conformity.

197
00:37:22.100 --> 00:37:42.019
Bas Overtoom: Maybe one thing I wanted to ask, I see the 6 to 8 weeks for Phase 1, and now we have only 5 more months for the first deadline. If you are not really started on this journey, is there also a way to do things faster, Papain? Can you maybe share a bit? I think some people might get nervous.

198
00:37:42.810 --> 00:38:02.289
Pepijn van der Laan: Yeah, so I think what's important to realize, it all depends also on your starting point, and I think getting that clarity, and there will be a lot of companies who have already started part of this work, so all the pre-work that has been done is always helping.

199
00:38:02.340 --> 00:38:10.040
Pepijn van der Laan: And if we have, limited complexity, then we can, can of course do,

200
00:38:10.310 --> 00:38:20.029
Pepijn van der Laan: do things faster, but it's good to realize that in that first phase, we'll also be, be looking at some of the product information, and…

201
00:38:20.500 --> 00:38:35.580
Pepijn van der Laan: require… and getting all the, all the relevant information may… may take some time to, to mobilize, and we are a bit, careful here in the, in the estimate. The biggest accelerator towards compliance is,

202
00:38:35.580 --> 00:38:42.559
Pepijn van der Laan: I believe in the, in the later part of that, that journey, if you have, already more,

203
00:38:42.790 --> 00:38:54.700
Pepijn van der Laan: They have more controls in play, things that you can leverage, and there you can also scale up the speed faster, as soon as you have the clarity on the roadmap and on the

204
00:38:55.300 --> 00:38:57.359
Pepijn van der Laan: On the definition of them.

205
00:38:57.920 --> 00:39:01.529
Bas Overtoom: Yeah, and I think starting now is still a good timing, and if you wait.

206
00:39:01.530 --> 00:39:03.430
Pepijn van der Laan: Still, it's still a good time, boss.

207
00:39:03.430 --> 00:39:11.950
Bas Overtoom: Yeah, then it will get, really get difficult also for us to support you with the resources limitations that we have.

208
00:39:12.010 --> 00:39:33.690
Bas Overtoom: Okay, yeah, then maybe closing close to the Q&A. We have over 20, almost 30 questions already come in, so I'm not sure we can handle all of them, but we will do our best in the minutes that is, that is left, here. Maybe a few short, call-to-actions. If you like this webinar, we will do another one on the

209
00:39:33.690 --> 00:39:37.520
Bas Overtoom: 8th of April, led by Danielle and the team.

210
00:39:37.520 --> 00:39:44.159

Bas Overtoom: that goes much more into some of the latest updates on the EU developments.

211
00:39:44.160 --> 00:40:08.400
Bas Overtoom: on the standards and regulations that will become some news on… in the coming days. I will give you an update there on the 8th of April. As a follow-up for this webinar, we will send you early next week a thank-you email with all the slides that you have here, and the replay of the video, but also a link to join this webinar. So you cannot register now, but from next week, early on, you can.

212
00:40:08.400 --> 00:40:18.420
Bas Overtoom: So that is really also a step to bring, let's say, one step deeper into the things that we already shared. So that's one of the things we're offering, but I can also imagine that

213
00:40:18.420 --> 00:40:35.670
Bas Overtoom: You don't want to wait yet another month before you want to get started, and for that, we offer to you as webinar participants an opportunity to talk with one of our experts, persons like Daniel or Papain, or the other experts that we have on this topic.

214
00:40:35.670 --> 00:40:49.019
Bas Overtoom: for an, yeah, let's say, a personalized dialogue. It will be a short call, of course, but to help you further on, on this journey, and to also shape a little bit what's going on. So if you think, hey.

215
00:40:49.020 --> 00:41:01.220
Bas Overtoom: I cannot wait till April. We want to get going. Please sign up here, register for this call, and we'll get back to you and start to plan that in and roll things out.

216
00:41:01.300 --> 00:41:23.740

Bas Overtoom: Last but not least, I just wanted to mention that we have also a very active LinkedIn group, where we post regular on CIA, on CRA, sorry, also on AI, we have many insight and news. We also do many of these kind of webinars on different kind of topics, so if you're not already a member, this is also a great way to kind of get going in that digital

217
00:41:23.750 --> 00:41:29.619
Bas Overtoom: journey. So that has kind of the concrete actions. Now, let's dive into…

218
00:41:30.370 --> 00:41:47.360
Bas Overtoom: the… yeah, the Q&A and the questions that came. So, yeah, just to get ready, I think I saw… I peeked already a little bit into some of the questions that were coming, and I saw that one question was… came up quite a bit.

219
00:41:47.360 --> 00:41:53.409
Bas Overtoom: And that is the question, and we mentioned a little bit on it, but it wasn't the question on the other…

220
00:41:54.060 --> 00:42:12.009
Bas Overtoom: the arrival of the horizontal standards, and when do we know more about it, is basically the question. What is the timeline that we can share on those standards? Maybe, Papane, you had a slide on that, maybe you can speak a bit to that, and then I also want to segue to

221
00:42:12.120 --> 00:42:18.050
Bas Overtoom: Daniel, because I know that you're heavily monitoring this, so maybe you can peek a bit on that, on that.

222
00:42:18.050 --> 00:42:18.840
Pepijn van der Laan: Yeah, I think.

223
00:42:18.840 --> 00:42:19.550
Bas Overtoom: Question.

224
00:42:20.200 --> 00:42:39.509
Pepijn van der Laan: Yeah, so I think it's, yeah, it's of course a good, a good, and relevant, and relevant question. So there's already a number of, a number of standards that are, that are currently, inquiry or under, under votes. So, for example, the, the, the.

225
00:42:39.510 --> 00:42:45.810
Pepijn van der Laan: the 40,001, series of standards.

226
00:42:45.810 --> 00:42:56.410
Pepijn van der Laan: Which is horizontal standards that, that you can already look at when it comes to vulnerability handling, when it comes to

227
00:42:56.470 --> 00:43:15.019
Pepijn van der Laan: has some of the general, principles and, and requirements also around, at a risk mo- risk, management, process. So there, there are standards, available. There are also standards which are still, in the process of, of being drafted.

228
00:43:16.260 --> 00:43:32.650
Pepijn van der Laan: also a number of vertical standards for specific product categories already being, being released out of, out of Etsy. So, of course, it's very important, depending on the type of product, which, which standard you, you look at.

229
00:43:32.650 --> 00:43:44.460
Pepijn van der Laan: But there's, yeah, quite a lot of, development here, which we are closely monitoring in order to make sure that we use the latest available information.

230

00:43:44.460 --> 00:44:00.100
Pepijn van der Laan: And of course, this is a bit of a squeeze, yeah, because, yeah, if you want to prepare, yeah, you want to wait for the standards. On the other hand, yeah, if standards are not there, yeah, it's also not an excuse to basically sit and wait, because there's already quite a bit that we

231
00:44:00.100 --> 00:44:12.109
Pepijn van der Laan: that we know is there, and that you can start working towards. In particular, if you know that you have quite a gap to fill. But Daniel, maybe you can add to that.

232
00:44:13.300 --> 00:44:19.440
Daniel Havre: Yeah, yeah, so as you said, there is a lot of development in these standards, so many of the…

233
00:44:19.800 --> 00:44:28.760
Daniel Havre: welcome standards, I mean, the developers are mainly the San Lect Gatsys who are developing these types of standards, and

234
00:44:29.180 --> 00:44:48.960
Daniel Havre: Many of them, especially from the Etsy, do have a publication goal of, I think it's end of October this year, or somewhere late this year. So hopefully, that date will be,

235
00:44:49.390 --> 00:45:03.089
Daniel Havre: the actual date, time will tell, but yeah, as, Papen said, it's, it's currently, in, in, draft or during development, as of today, yeah. Yeah.

236
00:45:03.490 --> 00:45:20.160
Pepijn van der Laan: Yeah, maybe related to this, I saw there was another question also about some of the exemptions of product categories, like medical devices. Maybe good

to mention that this is specifically for product categories that have already their own set of standards.

237
00:45:20.210 --> 00:45:29.450
Pepijn van der Laan: so that, this is not going to be basically conflicting with existing, regulations. So that's the background there.

238
00:45:30.830 --> 00:45:31.220
Bas Overtoom: Yeah.

239
00:45:31.220 --> 00:45:41.199
Daniel Havre: But this is not covering all, just want to add on to that, and it's, yeah, for medical in vitro, aviation and such, you are,

240
00:45:41.590 --> 00:45:50.749
Daniel Havre: by default out of scope, but there are other cybersecurity regulations which will go in parallel as well with the Cyber Resilience Act.

241
00:45:52.170 --> 00:46:11.589
Bas Overtoom: Maybe giving a little bit of insight on the numbers, I think that's also interesting, but remember the poll we filled in earlier, so… yeah, I think 60%, they are either in 1 or 2, that means teach me everything, or we really need structure and support. So that is only ever counted up at 70% in total, so…

242
00:46:11.750 --> 00:46:30.160
Bas Overtoom: That is basically, I think, 70% of you guys, they are, yeah, you're in the earlier journey, then there's another 25% that is, hey, we think we have it covered, we think we're there. This is more of a sanity check, and looking into the details, so, great job for you, 25% of the audience.

243

00:46:30.160 --> 00:46:44.719
Bas Overtoom: And then the last 5%, which is really the top dogs here, we're almost there, or hey, we feel we have it covered, we are just kind of browsing and there. So they're kind of the kings here of the room. So this gives a bit of an indication

244
00:46:44.720 --> 00:46:53.459
Bas Overtoom: where you are, and I think it gives also a bit of an indication on you and the audience, yeah, how fast you need to get going. So if you're in the bottom 70%,

245
00:46:53.460 --> 00:47:12.290
Bas Overtoom: then you are… today is the moment to make action in the journey that we talked about earlier. I can pick up another 3 or 4 questions. We have 30 plus, so we cannot have everything, but we will try to answer every question by email, or please also sign up for that individual call that we have offered.

246
00:47:12.290 --> 00:47:26.589
Bas Overtoom: For all of you. Maybe the difference between RED and CRA? I'm RED certified. What do I need to still do? I think, Daniel, you're nodding. This is typically something that you get this question a lot. Maybe you can clarify it a bit.

247
00:47:27.220 --> 00:47:44.619
Daniel Havre: Yeah, so, the CRA includes basically three types of requirements. It's the procedural requirements regarding vulnerability handling, and the secure design requirements. So those will be new additional requirements.

248
00:47:45.160 --> 00:47:51.010
Daniel Havre: But it also includes the product-specific requirements, and…

249
00:47:51.620 --> 00:48:09.849

Daniel Havre: Based on the essential requirements that we see in the CRA, there can be a mapping to what the RED or the EN18031 series will cover with the, with the, essential requirements of the CRA. So,

250
00:48:10.150 --> 00:48:24.590
Daniel Havre: We usually like to say that for the product-specific requirements, if you satisfy the EN18031, you are approximately satisfying about 80%, maybe more or less, depending on what type of product you have.

251
00:48:24.810 --> 00:48:34.440
Daniel Havre: By complying to the Red Cyber. So the Red Cyber is only focusing on the product itself, but nothing about the…

252
00:48:34.990 --> 00:48:40.940
Daniel Havre: Vulnerability handling, or how it is being developed, so that's additional requirements for some…

253
00:48:40.940 --> 00:49:00.309
Bas Overtoom: So part of the software and the connected devices need to be included in CRA also, definitely, yeah. So, and does that count for all the classes, Daniel, or is that also for, let's say, let's say, the non-critical, non-important, products, or the lower, let's say, risk, less risky products they are…

254
00:49:00.400 --> 00:49:03.310
Bas Overtoom: excluded. Could you shine a light on that?

255
00:49:03.910 --> 00:49:10.539
Daniel Havre: Yeah, so, I mean, if you are in the critical, class, there will be…

256
00:49:10.780 --> 00:49:19.110

Daniel Havre: stricter requirements depend, since you are in, in the stricter, class, which…

257
00:49:19.270 --> 00:49:23.250
Daniel Havre: Will of course, affect that,

258
00:49:24.620 --> 00:49:35.670
Daniel Havre: those type of requirements. But the overall view, looking at the essential requirements of the, Cyber Resilience Act.

259
00:49:35.800 --> 00:49:54.730
Daniel Havre: as I briefly mentioned when I showed the requirements as well, you do have your requirements regarding confidentiality, integrity, authenticity, access control mechanism updates, etc, etc. These are all elements that are being addressed in the EN18031, so if you do have secure

260
00:49:54.730 --> 00:50:01.119
Daniel Havre: implementation today by following that standard. It's safe to assume that,

261
00:50:01.470 --> 00:50:06.560
Daniel Havre: It's a high possibility that you will satisfy, the coming requirements.

262
00:50:07.090 --> 00:50:15.009
Bas Overtoom: And what if this is, of course, for new products that you're bringing to market, but let's say the product categories that you have already on the market, they… you need to kind of still…

263
00:50:15.540 --> 00:50:21.159
Bas Overtoom: certify them all for CRA, do I understand that correctly? Okay, yeah, that's your.

264
00:50:21.160 --> 00:50:31.250
Daniel Havre: Or, or, or, I mean, products that you have on the market today is not, it's… but if you continue to sell them after

265
00:50:31.600 --> 00:50:40.789
Daniel Havre: the 11th of December, then the same product, if you continue to sell the same product after 11th December 2027, they need to comply.

266
00:50:41.640 --> 00:50:53.290
Bas Overtoom: a market release date, it doesn't matter, it is the moment, yeah, if you want to continue selling, that is when it is. Maybe try to combine two questions, and then we need to slowly round off, also,

267
00:50:53.290 --> 00:51:05.450
Bas Overtoom: Here, Papayne, maybe two questions that are similar. They're not similar, but I think you can both speak a bit to it. One is more on, how do you execute a gap assessment when the standards are not there?

268
00:51:05.510 --> 00:51:20.600
Bas Overtoom: So what do you gap against? And another question, which is, I think, related to the organizational part, like, hey, ISO 27001 on processes, yeah, and how much do we then have covered that embedding part already? Maybe you can speak a bit to those,

269
00:51:20.680 --> 00:51:21.560
Bas Overtoom: those things.

270
00:51:21.560 --> 00:51:22.100
Pepijn van der Laan: Yeah.

271
00:51:22.190 --> 00:51:38.699
Pepijn van der Laan: Exactly. So, basically, if you do… thinking about, about 27,000, maybe first, that, of course, is, is purely, a process, lens, towards, towards the management system.

272
00:51:38.700 --> 00:51:48.910
Pepijn van der Laan: So that is going to help you a lot, because you will have a lot of structure and a lot of the base processes already in place.

273
00:51:48.940 --> 00:52:00.920
Pepijn van der Laan: On top of that, there are a couple of elements which are quite specific for the CRA regulations, in terms of what they want to… what you want to see in

274
00:52:00.920 --> 00:52:20.010
Pepijn van der Laan: For example, the, the risk assessments that we're talking about, yeah, where… because this is, less focused on the organization and no goals as well, but much more on the, on the protection goals also from, from a regulation perspective, so that's a different lens.

275
00:52:20.010 --> 00:52:22.789
Pepijn van der Laan: So that leads to a bit of,

276
00:52:22.790 --> 00:52:32.600
Pepijn van der Laan: of a gap or additional requirements that you will need to take into account. Still, it's going to help you massively to get towards the…

277
00:52:33.610 --> 00:52:35.150
Pepijn van der Laan: Head towards the…

278
00:52:35.790 --> 00:52:51.470
Pepijn van der Laan: towards compliance. So, and then about doing a gap when, yeah, when the, when the goalposts are still, are still moving. Yeah, this is, of course, something where we lean on.

279
00:52:51.820 --> 00:53:11.669
Pepijn van der Laan: two types of input, yeah. One is the harmonized standards that are there, and in particular, at this moment, the draft standards, because they're not harmonized yet, so that means those harmonized standards already give a good indication of what to expect.

280
00:53:11.670 --> 00:53:16.210
Pepijn van der Laan: So, there we can also, in the gap, in the gap assessment.

281
00:53:16.210 --> 00:53:24.549
Pepijn van der Laan: indicate where do we have a clear view of where things are going, and where are still the question marks. So that you also get a clear view on what can we…

282
00:53:24.590 --> 00:53:29.890
Pepijn van der Laan: Confidently work towards, and what are basically the no-regret moves that you can already make.

283
00:53:29.990 --> 00:53:36.409
Pepijn van der Laan: And also indicate, yeah, where would we really advise to wait for additional guidance?

284
00:53:36.520 --> 00:53:50.760

Pepijn van der Laan: Before you can make a different choice. And that's… and where those points are, yeah, this also is often very dependent on the specific situation, what are the type of products you have? What are the… what is the…

285
00:53:51.280 --> 00:53:59.779
Pepijn van der Laan: the states where the standards are for those type of products, but also, yeah, what are the specific concerns you have? Is it about

286
00:53:59.820 --> 00:54:12.319
Pepijn van der Laan: a lot of external, suppliers that you have to basically combine into one, into one, SBOM? Or is it much more about,

287
00:54:12.680 --> 00:54:26.520
Pepijn van der Laan: basically other elements, like, yeah, like the vulnerability handling, where you, where you are concerned. So, that depends a lot on those type of elements, and there we can, yeah, can help you create the clarity in your situation.

288
00:54:27.330 --> 00:54:34.679
Bas Overtoom: Okay, yeah, it is time for the last question. Sorry, we haven't been able to, to, to answer all of them, but I…

289
00:54:34.680 --> 00:54:51.990
Bas Overtoom: where we can, we will try to contact you by email, or please fill in the QR code for the call. I will put it on screen in a minute, so you can… in case you missed it, but maybe just do a quick 2 minutes on the last question, because it came a bit… came up quite a bit.

290
00:54:51.990 --> 00:55:10.410
Bas Overtoom: It is basically on that vulnerability reporting. So, where do we need to report vulnerabilities? What do we need to communicate to our customers? Basically,

that first kind of requirement. What is a bit… can we shine a bit of a light of that definition on them? Maybe, Daniel, you can share some initial

291
00:55:10.410 --> 00:55:14.660
Bas Overtoom: Yeah, let's say views, and then Papana gives you the last word before we close off.

292
00:55:16.540 --> 00:55:27.950
Daniel Havre: Yeah, so, there will be a, reporting platform, which Anissa will, Handle, basically.

293
00:55:28.050 --> 00:55:33.689
Daniel Havre: So you need to… Report… let's see…

294
00:55:34.170 --> 00:55:39.609
Daniel Havre: You need to report actively exploitable vulnerabilities.

295
00:55:39.860 --> 00:55:58.259
Daniel Havre: And that includes, also, severe security incidents. So, that needs to be, reported. And there will be a NISA site where you do.

296
00:55:58.460 --> 00:56:03.380
Daniel Havre: Where you shall have the, availability to, to, report this.

297
00:56:05.130 --> 00:56:23.250
Pepijn van der Laan: Yeah, and the 11th of September is really the key data when the, when the requirement comes into, comes into action. So, so that is really the, yeah, the day to monitor towards, yeah, towards the setup also of that, of that portal.

298

00:56:23.830 --> 00:56:42.979
Bas Overtoom: Yeah, and then a question comes in, I think that's interesting. Do you think I can do it myself, or do I need a consultant? Now, I think that answer is basically up to all of you, to figure it out. We're here to share at least our information in a webinar like this, the one coming up on the 8th of April, also here.

299
00:56:42.980 --> 00:57:01.619
Bas Overtoom: Again, the QR code, if you want to speak further and make things concrete, we are available to try to shape a project in the way we could support you anywhere on the line of that journey, but I think else it would be… I hope this was relevant content for you to kind of form your own,

300
00:57:01.620 --> 00:57:05.960
Bas Overtoom: journey, if so required. So that is also possible.

301
00:57:05.960 --> 00:57:13.549
Bas Overtoom: I would like to thank you, there's also the link in the chat for people that couldn't get their phones out quick enough.

302
00:57:13.550 --> 00:57:37.410
Bas Overtoom: I would like to thank you, Papain, for sharing your light on the, kind of, the overview. I'd like to thank you, Danielle, for sharing also your, kind of, very pragmatic and hands-on insights on the testing and the nitty-gritty on some of the requirements, making also that link with RED, which is for a lot of our clients, basically.

303
00:57:37.410 --> 00:57:43.010
Bas Overtoom: yeah, station that they have, have already passed, so that, I think, gives you a huge advantage.

304
00:57:43.010 --> 00:57:52.929

Bas Overtoom: to become ready for the 11th of September, which is quite quick. We have also the summer in between, at least for us in Europe, that means,

305
00:57:52.930 --> 00:58:10.499
Bas Overtoom: 6 weeks of more relaxed, things, so yeah, that makes the time even shorter. So, now, good luck to everybody. We are here to help. So, love to hear from you, and, thank you again, and we wish you a beautiful, day. Thank you all.

306
00:58:11.520 --> 00:58:12.410
Daniel Havre: Thank you.

307
00:58:13.170 --> 00:58:13.930
Pepijn van der Laan: Thank you.