OWASP
NEW
ZEALAND
owasp.org.nz

State of AppSec in New Zealand

2022 Survey Report

Volume 2 – Response Data

Contents

INTRODUCTION 3

SURVEY STRUCTURE 4

Personal and Demographic Information Collected 4
Duplicate Responses 4
Test / Fake / Blank Responses 5
Multiple Organisation Responses 5

DATA COLLECTION AND CLEAN-UP 6

DETAILED RESPONSES 7

Demographic Information 7

Organisation Type 8

Governance, Risk, and Compliance 8

Security Requirements 9

Penetration Testing 12

OWASP Awareness and Use 13

Application Security Program 13

Software Development Practices 15

Security Testing 15

Deployment and DevOps 16

Logging and Monitoring 18

Security Training 18

Bug Bounties 19

Cloud Security 19

Technology Skills 20

ACKNOWLEDGEMENTS 22

Introduction

This document comprises the second volume of OWASP®* New Zealand's report on the first annual State of AppSec in New Zealand Survey. In this volume, we present information on the survey's structure and design, along with a complete listing of the questions presented in the 2022 survey, and the responses received.

This document is a companion to the first volume, which provides an overview of and commentary on the survey and its responses.

Both documents can be found on the OWASP® New Zealand Chapter's website at: https://owasp.org/www-chapter-new-zealand.

* 'OWASP' is a registered trademark, and the OWASP New Zealand logo is a trademark, of the OWASP Foundation, Inc.
Unless otherwise specified, information in this document is provided without warranty of service or accuracy. For more information, please refer to our General Disclaimer.

Survey Structure

In designing the survey, the project team sought to account for the fact not every organisation approaches software development / acquisition in the same way. The team's objective was to obtain responses from a wide variety of organisations throughout New Zealand, capturing their perspectives on application security, whether or not they develop software themselves.

To this end, the team created a dynamic survey, where each respondent is presented one of four series of survey pages, based on the general nature of their approach to software development and deployment. In response to the question "Which of the following statements best describes your organisation?" the respondent was required to select one of the following options:

- We use only "off-the-shelf" commercial software
- All our development and deployment of custom applications is outsourced
- We outsource development, and deploy applications in our own environment
- We develop applications in house

Based on their response to this question, the respondent was then presented with a different subset of the survey's questions. For questions presented to only a portion of the respondents, the number of responses received was significantly less than the total.

Personal and Demographic Information Collected

While the survey results are fully anonymised, it was necessary to collect a small amount of personal information from respondents. The purposes for which this information was collected were: to identify multiple responses submitted by the same individual; to eliminate test/fake responses and those not associated with any organisation; and to identify responses submitted by multiple individuals from the same organisation.

After agreeing to the Privacy Statement, respondents were asked for three (3) items of identifying information:

1. Their Name
2. The Organisation for which they work
3. Their role within the organisation

Additionally, at the end of the survey, each respondent was asked if they were willing to be contacted by the project team, for clarification or follow-up on their responses. If they answered 'yes' to this question, they were then asked to provide their preferred contact e-mail address and phone number.

Respondents' names and contact information have been used only for the purposes described herein, and have not been shared with anyone outside the project team.

Duplicate Responses

The survey process did not support respondents' returning to edit their previously submitted responses. A respondent wishing to update their response had to complete the

full survey again, resulting in multiple submissions by the same respondent. In this event, only the last submitted response was retained in the final data set.

Test / Fake / Blank Responses

After the survey was published and the first response received, it was no longer possible to clear the response data set. If a project team member needed to verify the correct behaviour of the live survey, they would visit the survey site. Each time this was done, a new 'submission' was added to the raw data set. These 'test' records were excluded from the final data set.

Similarly, any time someone visited the survey site and began a response, or simply had a look around and left the site – a record was added to the raw data set. The resulting 'false-start' response records – where no questions were actually answered, or some or all of the required identifying information was not supplied – were excluded from the final data set.

Multiple Organisation Responses

The objectives of the survey require at most one answer to each question from each responding organisation. In those cases where more than one individual submitted a response for a given organisation, these responses needed to be reconciled and consolidated into a single response.

For each survey question and for a given organisation, one of three possible situations could arise with multiple responses:

- Only one of the respondents provided an answer to the question – In this case, the single answer provided was retained;
- Multiple respondents provided *the same* answer to the question – In this case, the common answer was retained; or
- Multiple respondents provided *different* answers to the question – In this case, the answer given by the majority of respondents was retained, with ties resolved by looking to the respondents' respective roles within the organisation. Among the tied answers, the one provided by the respondent with the most 'senior' role was selected.

Data Collection and Clean-up

The 2022 survey was published in mid-May, and the first response was submitted on the 24th of May. The survey remained open for responses through the 31st of July, with the last response recorded on the 18th of July.

A total of 91 responses were received. 17 responses were removed from the data set, due to meeting one or more of the following conditions:

- The response was superseded by a later response submitted by the same individual;
- The response did not contain an organisation name;
- The response was completely blank; or
- The response contained an intentionally invalid name (e.g., "Test User").

Of the 74 individual responses remaining, 45 were the singular response for an organisation. An additional 11 organisations were represented by two (6 organisations), three (3 organisations), or four (2 organisations) responses, accounting for the remaining 29.

After consolidating multiple responses, the final data set contained responses representing 56 distinct New Zealand organisations. This fell significantly short of the project team's target of at least 100 organisations in the final data set. Given the small overall sample size represented, caution should be exercised in basing conclusions or projections on the results presented herein.

For questions presented to only a portion of the respondents, the number of responses received was significantly less than the total. This should be recognised as a further limitation of the results presented herein – questions for which only a small number of responses were received are unlikely to be representative of New Zealand organisations on the whole and great care should be taken in basing inferences on those results.

Detailed Responses

Demographic Information

The demographic information reported in this section represents the individual responses from the 74 unique respondents retained in the final data set. The 2022 survey included two demographic questions on which data can be reported.

Question: What is your role?

NOTE: This was a free-text question, to which many respondents provided their actual job titles. To preserve anonymity, responses have been categorised and summarised.

Response	Count	Proportion
"C-Level" executive	3	4%
Management-Level, Security	7	10%
Management-Level, Development	6	8%
Management-Level, Other	3	4%
Non-Management, Security	24	32%
Non-Management, Development	27	36%
Non-Management, Other	2	3%
No Response	2	3%

Question: What responsibilities do you have at your organisation?

NOTE: Multiple responses were permitted

Response	Count	Proportion
I write code (developer)	31	42%
I deploy applications (operations)	21	28%
I manage teams that write and/or deploy applications	16	22%
I secure the applications my organisation creates	24	32%
I manage teams that secure the applications my organisation creates	9	12%
I secure my organisation more broadly	30	41%
No Response	5	7%

Organisation Type

As described above, each respondent was required to select one of four options for their organisation's approach to developing or acquiring software.

Question: Which of the following statements best describes your organisation?

NOTE: This question required a response, before the respondent could proceed further. For this reason, every response included in the final data set contained an answer to this question.

Response	Count	Proportion
We only use "off-the-shelf" commercial software	6	11%
All of our development and deployment of custom applications is outsourced	5	9%
We outsource development, and deploy them in our own environment	4	7%
We develop applications in-house	41	73%

Governance, Risk, and Compliance

Question: Do you have a list of all your applications, especially your critical ones?

Response	Count	Proportion
Yes, we have a complete list and know which applications are critical	20	36%
Yes, but the list is incomplete	17	30%
Yes, but our applications are not prioritised	9	16%
No	4	7%
I don't know	2	4%
No Response	4	7%

Question: From your list of applications, do you map the dependencies of the applications? (Software supply chain management / SCA)

Response	Count	Proportion
Yes	22	39%
No	12	21%
I don't know	7	13%
No Response	15	27%

Question: Do you classify applications according to business risk?

For this question, respondents selected a value between 0 and 100 using a slider. A value of zero (0) indicated the organisation never does this, while a value of 100 indicated the organisation applies the risk classification process to every application.

Of the 56 organisations, five (5) provided no response to this question. Among the 51 organisations providing a response, the average value selected was **65 out of 100**.

Question: Do you have a Cyber Policy that supports Application Security?

Response	Count	Proportion
Yes, we have a specific AppSec Policy	7	13%
Yes, AppSec is included in broader Cyber Security policies	1	2%
No	3	5%
I don't know	4	7%
No Response	41	73%

Question: Do you maintain a Risk Register?

Response	Count	Proportion
Yes, in an application	19	34%
Yes, in a spreadsheet	20	36%
Partially, in emails or similar formats	5	9%
No	5	9%
I don't know	4	7%
No Response	3	5%

Question: Do you have a vulnerability and patch management program for your customised applications? (not just your infrastructure and OS)

Response	Count	Proportion
Yes	26	46%
It's a work in progress	15	27%
No	7	13%
I don't know	2	4%
No Response	6	11%

Security Requirements

Respondents were asked how they go about defining security requirements for their applications. The wording of the question varied, based on the organisation type. However, the response choices were the same across all variants.

Question (off-the-shelf software): How do you define security requirements for choosing your applications? [6 organisations]

Response	Count	Proportion
Based on a requirements framework	3	50%
Based on standards and/or regulatory compliance	1	17%
We perform threat modelling exercises	1	17%
Based on the knowledge of our team members	1	17%
We don't define security requirements	0	0%
I don't know	0	0%

Question (outsourced development): How do you define security requirements for outsourcing the development of your applications? [9 organisations]

Response	Count	Proportion
Based on a requirements framework	1	11%
Based on standards and/or regulatory compliance	3	33%
We perform threat modelling exercises	1	11%
Based on the knowledge of our team members	1	11%
We don't define security requirements	2	22%
I don't know	1	11%

Question (in-house development): How do you define security requirements? [41 organisations]

Response	Count	Proportion
Based on a requirements framework	3	7%
Based on standards and/or regulatory compliance	21	51%
We perform threat modelling exercises	8	20%
Based on the knowledge of our team members	8	20%
We don't define security requirements	1	2%
I don't know	0	0%

Consolidated Responses:

Response	Count	Proportion
Based on a requirements framework	7	13%
Based on standards and/or regulatory compliance	25	45%
We perform threat modelling exercises	10	18%
Based on the knowledge of our team members	10	18%
We don't define security requirements	3	5%
I don't know	1	2%

Respondents were next asked how their security requirements are validated. Both the wording of the question and the available responses varied, based on the organisation.

Question (off-the-shelf software): How are security requirements validated? [6 organisations]

Response	Count	Proportion
We perform our own testing for security requirements	2	33%
We perform external penetration tests	2	33%
The vendor attestation is sufficient	0	0%
There is no defined process to validate security requirements	1	17%
Other	1	17%
I don't know	0	0%

Question (outsourced development): How are those security requirements validated? [9 organisations]

Response	Count	Proportion
We perform our own testing for security requirements	2	22%
We perform external penetration tests	2	22%
The vendor attestation is sufficient	2	22%
There is no defined process to validate security requirements	1	11%
Other	1	11%
I don't know	1	11%

Question (in-house development): How are security requirements validated? [41 organisations]

Response	Count	Proportion
We create specific tests to validate our defined security requirements	13	32%
Based on penetration test results	18	44%
There is no defined process to validate security requirements	7	17%
Other	3	7%
I don't know	0	0%

For organisations using only off-the-shelf software, or outsourcing development of applications, respondents were also asked how they ensure delivered applications are secure. Wording of the question and the response selections were slightly different for the two scenarios.

Question (off-the-shelf software): How do you ensure that applications you purchase are secure? [6 organisations]

Response	Count	Proportion
We purchase only from vendors we feel are trustworthy	3	50%
We test all applications in-house or have them tested by a third party	2	33%
We ask for compliance reports based on industry standards	1	17%
We have a third-party security review process based on a questionnaire	0	0%
I don't know	0	0%

Question (outsourced development): How do you ensure that the applications you have developed are secure? [9 organisations]

Response	Count	Proportion
Based on a requirements framework	1	11%
We test all applications in-house or have them tested by a third party	4	44%
We ask for compliance reports based on industry standards	2	22%
We have a third-party security review process based on a questionnaire	1	11%
I don't know	1	11%

Penetration Testing

In this group of questions, respondents were asked about their organisations' penetration testing practices, including whether and how the results of penetration tests are acted upon within the organisation.

Question: What is your approach to penetration testing?

Response	Count	Proportion
We perform penetration testing at a regular cadence based on criticality of the applications	31	56%
We perform penetration testing only for new applications	1	2%
We perform penetration testing to meet compliance requirements	7	12%
We perform *ad hoc* penetration testing	4	7%
We don't perform penetration testing	6	11%
No response	7	12%

Question: What do you do with the results of penetration tests?

Response	Count	Proportion
Remediate everything prior to deployment	9	16%
Remediate findings only if they're critical	20	36%
Feedback to the development teams to understand root-cause and limit issues in the future	12	21%
File the report	0	0%
Do nothing	0	0%
No response	15	27%

OWASP Awareness and Use

In this group of questions, respondents were asked about their awareness of OWASP® (the Open Worldwide [formerly Web] Application Security Project) and their use of OWASP® tools.

Question: Have you heard of the OWASP organisation? (Open Web Application Security Project)

Response	Count	Proportion
Yes, and we use tools from OWASP	7	13%
Yes, we have heard of OWASP, but we don't use any tools	7	13%
No	0	0%
No response	42	75%

Question: Do you use OWASP tools? If yes, which of these popular tools do you use?
NOTE: Multiple responses were permitted

Response	Count	Proportion
OWASP Top 10	19	34%
Cheat Sheets	11	20%
Security Testing Guides	9	16%
Zed Attack Proxy (ZAP)	8	14%
Dependency Track	5	9%
Software Assurance Maturity Model (SAMM)	3	5%
Application Security Verification Standard (ASVS)	2	4%
Amass	1	2%
Dependency Check	1	2%
ModSecurity with OWASP Core Rule Set (CRS)	1	2%
Dependency Check	1	2%
Defect Dojo	0	0%

Application Security Program

In this group of questions, respondents were asked about their organisations' application security programs, including the level of support and funding they receive.

Question: Do you feel your organisation prioritises AppSec?

For this question, respondents selected a value between 0 and 100 using a slider. A value of zero (0) indicated they feel their organisation doesn't prioritise AppSec at all, while a value of 100 indicated their organisation prioritises it above all else.

Of the 56 organisations, 9 provided no response to this question. Among the 47 organisations providing a response, the average value selected was **66 out of 100**.

Question: Do you have an Application Security program? (an AppSec program is a defined set of projects to improve the security of applications that you develop and/or manage)

Response	Count	Proportion
Yes	14	25%
Partial, AppSec is a responsibility of wider security team	9	16%
Partial, AppSec is a responsibility of development teams	10	18%
No, there isn't an AppSec program	5	9%
I don't know	2	4%
No Response	16	29%

Question: Are you looking to implement an AppSec program in the next 12 months?

Response	Count	Proportion
Yes	13	23%
No	12	21%
No Response	31	55%

Question: How do you fund the AppSec Program?

Response	Count	Proportion
We have a defined budget specifically for AppSec	4	7%
It is part of a broader Cyber security budget	13	23%
It is part of a broader development budget	6	11%
We don't have a defined budget	1	2%
Funding is obtained on an *ad-hoc* basis	0	0%
AppSec is funded only if we get hacked	0	0%
I don't know	4	7%
No Response	28	50%

Question: Do you report the state of AppSec to senior leadership?

Response	Count	Proportion
Yes, it is presented to senior leadership on a regular basis	11	20%
Yes, it is presented on an *ad-hoc* basis	9	16%
It comes up when something goes wrong	3	5%
No, we don't report on AppSec	3	5%
I don't know	2	4%
No Response	28	50%

Software Development Practices

In this question group, respondents were asked questions related to their organisations' software development and secure coding practices.

Question: What development process does your contractor follow?

NOTE: This question was erroneously asked only to respondents whose organisations outsource development, but manage deployment and operations in-house. [4 organisations]

Response	Count	Proportion
Agile	4	100%
Waterfall	0	0%
Lean	0	0%
I don't know	0	0%
No Response	0	0%

Question: Do you have a secure coding standard?

Response	Count	Proportion
Yes	30	54%
No	6	11%
I don't know	3	5%
No response	17	30%

Question: How confident are you in your process to identify security design flaws prior to testing?

For this question, respondents selected a value between 0 and 100 using a slider. A value of zero (0) indicated no confidence, while a value of 100 indicated total confidence.

Of the 56 organisations, 21 provided no response to this question. Among the 35 organisations providing a response, the average value selected was **61 out of 100**.

Security Testing

In this question group, respondents were asked about their organisations' security testing practices.

Question: Is security testing a part of the development phase?

Response	Count	Proportion
Yes	18	32%
Partially	12	21%
No	7	13%
I don't know	1	2%
No response	18	32%

Question: Which of the following testing methodologies do you use during the development phase?
NOTE: Multiple responses were permitted

Response	Count	Proportion
Test scripts to verify security requirements	23	41%
Automatic testing for security regressions	20	36%
Randomisation or Fuzzing	8	14%
Abuse case testing, from functional requirements	11	20%
DOS and Security denial of service	5	9%
I don't know	6	11%

Deployment and DevOps

Question: Which of these practices do you use to deploy your applications?
NOTE: Multiple responses were permitted

Response	Count	Proportion
Automation (CI/CD)	32	57%
Infrastructure as Code (IaC)	29	52%
Cloud Native tools	22	39%
Containers	29	52%
Serverless / Function as a Service	21	38%
Secrets Management	26	46%
Application Security Testing (AST) tools	23	41%
Code Repositories	32	57%
Open-source dependency verification	23	41%
I don't know	3	5%

Question: Do you implement automated security checks in your deployment process?

Response	Count	Proportion
Yes, we have tools and we break builds based on testing	2	4%
Yes, we have tools and they are part of the build processes	22	39%
No	8	14%
I don't know	4	7%
No response	20	36%

Question: What techniques do you use to manage secrets?

Response	Count	Proportion
We use hardware security modules (HSMs) for secret management	7	13%
We always generate and synchronize secrets using a SaaS solution	19	34%
We always generate and synchronize secrets using an on-prem solution	4	7%
Our secrets are stored in the source code via configuration files	3	5%
I don't know	3	5%
No response	20	36%

Question: Are security tools (e.g., SAST, SCA) integrated into the CI/CD pipeline?

Response	Count	Proportion
Yes	23	41%
No	12	21%
We don't have CI/CD pipelines	1	2%
No response	20	36%

Question: Which of the following AppSec tools does your organisation utilise?
NOTE: Multiple responses were permitted

Response	Count	Proportion
SAST - detects issues in the code we write	21	38%
DAST - detects issues in a running application	13	23%
IAST - detects issues by monitoring the testing process	7	13%
SCA - detects issues in third-party libraries used	16	29%
Web Application Firewall - sits in front of the application to protect against attacks	28	50%
Application Risk Management - prioritises remediation of vulnerabilities and exposures	15	27%
Operating System / Network Vulnerability scanner	25	45%
Cloud Security Posture Management (CSPM)	20	36%
Infrastructure as Code (IaC) scanning	16	29%
Container scanning	22	39%

Logging and Monitoring

In this question group, respondents were asked about their organisations' basic approach to logging and whether the generated logs are monitored.

Question: How strong is your logging?

Response	Count	Proportion
Centralised logging	35	63%
We log only locally	8	14%
We don't do logging	2	4%
I don't know	5	9%
No response	6	11%

Question: Do you monitor those logs?

Response	Count	Proportion
We actively monitor	22	39%
We alert on thresholds/triggers	15	27%
We monitor *ad hoc*	3	5%
We don't monitor	4	7%
I don't know	0	0%
No response	12	21%

Security Training

In this question 'group,' comprised of a single question, respondents were asked if and how their organisations provide security training to developers.

Question: Do you provide security training to your developers? If yes, how?
NOTE: Multiple responses were permitted

Response	Count	Proportion
We run in-house training seminars	12	21%
We use third-parties to deliver training seminars	10	18%
We have access to a secure coding training platform with lab exercises	11	20%
We have access to a video-based training platform	14	25%
We send people to conferences and industry events	13	23%
We don't provide security training to our developers	6	11%
I don't know	5	9%

Bug Bounties

In this question 'group,' also comprised of a single question, respondents were asked if their organisations make use of a Responsible Disclosure or Bug Bounty program to identify vulnerabilities in their applications.

Question: Do you have a vulnerability disclosure or bug-bounty program?

Response	Count	Proportion
Yes, we have a formalised program	5	9%
Yes, we have an informal program	6	11%
No	18	32%
I don't know	7	13%
No response	20	36%

Cloud Security

In this question group, respondents were asked for information on their organisations' use of cloud computing platforms, including the use of automated security tools within those environments.

Question: Do you use cloud services to deploy your applications?

Response	Count	Proportion
Yes	43	77%
No	4	7%
No response	9	16%

Question: How do you manage your application workloads?

Response	Count	Proportion
Cloud only, with multiple cloud service providers	6	11%
Cloud only, with a single cloud service provider	8	14%
Hybrid, with multiple cloud service providers	19	34%
Hybrid, with a single cloud service provider	7	13%
On-premise only	1	2%
I don't know	3	5%
No response	12	21%

Question: How do you primarily configure your cloud infrastructure?

Response	Count	Proportion
Infrastructure as Code (IaC)	32	57%
Manually	9	16%
Mixture of IaC and manual configuration	1	2%
No response	14	25%

Question: Do you use security tools that are native to your cloud provider?

Response	Count	Proportion
Yes, we rely exclusively on native security tools available on the CSP's platform	10	18%
Yes, but we also deploy third-party security tools	23	41%
No, we only use third-party security tools	5	9%
No, we don't use any security tools to protect our cloud environment	1	2%
I don’t know	4	7%
No response	13	23%

Technology Skills

In this question group, respondents were asked whether their organisations perceive a technology skills shortage and, for those that do, what strategies they’re employing to address the resulting skills gaps.

Question: Do you feel there is a technology skills shortage in New Zealand?

Response	Count	Proportion	Proportion (excl. ‘No response’)
Yes	44	79%	96%
No	2	4%	4%
No response	10	18%	---

Question: What are the important skills needed? (skill gaps for the next 12 months)
NOTE: Multiple responses were permitted

Response	Count	Proportion
General information security	28	50%
Security operations	26	46%
Risk assessment and management	27	48%
Threat analysis	29	52%
Network security	18	32%
DevSecOps/AppSec	36	64%
Cloud Security	35	63%
Other (Diplomacy)	1	2%
Other (Supply Chain Risk Management)	1	2%
Other (Everything)	1	2%

Question: How are you addressing the skills shortage?
NOTE: Multiple responses were permitted

Response	Count	Proportion
We are able to hire internationally	20	36%
We are utilising third parties/contractors	29	52%
We are hiring more interns and graduates and providing training	26	46%
We are upskilling existing team members	33	59%
Other (Market recruitment)	1	2%
Other (We train developers)	1	2%
Other (Making do with what we have)	1	2%

Acknowledgements

DATACOM

The State of AppSec Survey Project team wishes to acknowledge the support provided by Datacom Systems Limited (NZ), without which this project would never have happened. Datacom provided access to their Survey Monkey subscription, which was used to create and deliver the survey. In addition, members of Datacom's Application Security Services team were granted "release time" to work on the Survey in 2022.

The project team also wishes to acknowledge the contributions of the following volunteers, who contributed significantly to the Survey's development and execution:

- Kevin Alcock
- Raafey Khan
- Amith Murthy
- John-Paul (JP) Sikking