

TACTICAL



AS102

TOOL MISUSE AND EXPLOITATION

Your agent has permissions. That is the entire point of it.

CYBER SECURITY THAT STOPS HACKERS

// 01 // WHAT IT IS

NOBODY BREAKS ANYTHING

The agent uses the access you granted, in a sequence you did not anticipate, because someone worked out how to ask.

GRANTED ACCESS

Every tool the agent touches is one you deliberately allowed.

UNANTICIPATED SEQUENCE

The order of the calls, not the calls themselves, produces the harm.

NO EXPLOIT

Nothing is bypassed. Someone worked out how to ask.

// 02 // HOW IT HAPPENS

THE TOOL CALL WAS ALLOWED. THE CONTEXT WAS NOT.

Permissions are granted per tool. Attacks arrive per chain. An agent that may query a database and may send an email can do something neither permission describes.

// PERMISSION VERSUS CHAIN

WHAT YOU GRANTED

MAY QUERY A DATABASE

MAY SEND AN EMAIL

WHAT THE CHAIN DOES

QUERIES THE DATABASE, THEN EMAILS THE
RESULT OUT

// 03 // THE STANDARD

ASIO2 IS THE LEAST EXOTIC RISK ON THE LIST

9 DEC 2025

PUBLISHED

100+

SECURITY PRACTITIONERS

RANKED 2ND

NEEDS NO VULNERABILITY

OWASP GenAI Security Project, Agentic Security Initiative.

// 04 // WHY SOUTH AFRICA

YOU ALREADY HAVE THE OBLIGATION

**1 JUN
2025**

IN FORCE SINCE

Joint Standard 2 of 2024 has been in force since 1 June 2025. It requires documented evidence of control testing, including vulnerability scans, penetration tests and simulated incidents, plus a maintained testing calendar.

// WHO IT APPLIES TO

BANKS	INSURERS	ASSET MANAGERS
RETIREMENT FUNDS	CREDIT RATING AGENCIES	CERTAIN FSPS

Applies to banks, insurers, asset managers, retirement funds, credit rating agencies and certain financial service providers.

// 05 // THE POINT

AN AGENT THAT CALLS TOOLS IS A SYSTEM

Nothing in Joint Standard 2 exempts it from the testing calendar. Most calendars were written before the agents existed, and nobody has gone back.

WHAT THE CALENDAR COVERS

THE SYSTEMS YOU LISTED

Scans, penetration tests and simulated incidents, on schedule, with evidence.

WHAT IT MISSES

THE AGENTS

Written before the agents existed, and nobody has gone back.

// 06 // THREE QUESTIONS FOR MONDAY

THREE QUESTIONS FOR MONDAY

01 WHICH TOOLS CAN EACH OF OUR AGENTS CALL?

02 WHO APPROVED THAT LIST, AND WHEN?

03 IS A SINGLE AGENT ON OUR TESTING CALENDAR?

THE CALENDAR ALREADY EXISTS. THE AGENTS ARE NOT ON IT.

WE DO NOT RUN SCANS. WE DEPLOY OPERATORS.

// THE NEXT STEP

A THIRTY MINUTE DISCUSSION.

A no-obligation discussion to understand your requirement and to provide guidance on how NEWORDER can assist. No deployment, no commitment.

[BOOK DISCUSSION →](#)

EMAIL [INFO@NEWORDERGROUP.NET](mailto:info@newordergroup.net) · WEB [WWW.NEWORDERGROUP.NET](http://www.newordergroup.net)

NEXT: ASIO3 IDENTITY AND PRIVILEGE ABUSE