SECURITY · GUIDE

The skills matrix *for security teams*

A security operation is only as strong as its weakest function. Guarding may be solid while incident response is thin, or the control room sharp while cyber awareness lags, and an attacker only needs one gap. As physical and digital security converge, the range of skills a team must hold has widened fast. A skills matrix maps capability across every security function, so a manager can see at a glance which are ready, which are stretched, and where the operation is exposed.

Dr Alex J. Martin-Smith
CMGR · MBA · LLM · DBA

Reading time 12 min · **Method** Upleashed 0 to 5 capability framework · **Updated** May 2026

THE SHORT ANSWER

A security skills matrix maps the team against the functions a modern operation depends on, manned guarding, control room and CCTV, access control, incident response, investigations, and increasingly cyber and information security, scored on a clear scale. Read each function's readiness: where cover is strong, where it is thin, and where licensing is due. In short: **it shows capability function by function, so the weakest link, the under-covered or lapsing area an incident would expose, is visible and fixable before it is tested.**

KEY TAKEAWAYS

- **Security is only as strong as its weakest function.** Map every function, since one thin area is the gap an incident finds.
- **Physical and cyber are converging.** The skill set has widened; the matrix must span guarding, control room and information security alike.
- **Readiness, function by function.** Read each function's cover as a dial, so the stretched and exposed ones stand out at a glance.
- **Licensing and currency matter.** Guarding and CCTV roles need valid licences; the matrix tracks them, not just the underlying skill.
- **Cover every shift.** A 24/7 operation needs each critical function staffed around the clock, not just on average.

START HERE

As strong as the *weakest function*

Security is a chain: an operation with excellent guarding but a thin incident response, or a sharp control room but no cyber awareness, is only as protected as its weakest link, because an adversary needs to find just one. So the question is not whether the team is broadly capable, but whether **every function is covered** to the level the threat demands. A skills matrix answers it by showing readiness function by function, exposing the weak link before it is tested.

Map the full range of functions

A modern security matrix spans more than guarding. It maps the **functions a layered operation depends on**: manned guarding and patrol, control room and CCTV monitoring, access control, incident and emergency response, investigations, and, increasingly, cyber and information security. As physical and digital threats converge, even front-line officers are expected to recognise digital risks, so the matrix must reflect the widened skill set rather than the narrow one of a decade ago.

Read each function's readiness

The insight is **per function**. A team total can look healthy while one critical function sits dangerously thin. Reading the matrix function by function, how many people are genuinely capable in the control room, in incident response, in cyber awareness, turns a vague sense of "we're well staffed" into a clear

readiness picture: this function is strong, this one is stretched, this one is exposed. That is what lets a manager direct training and recruitment at the weakest links rather than spreading effort evenly.

Track licences and round-the-clock cover

Two security-specific factors shape the matrix. **Licensing and currency**: many guarding and CCTV roles require valid licences and refreshers, so the matrix tracks not just whether someone has a skill but whether their licence is current. And **round-the-clock cover**: a security operation typically runs 24/7, so each critical function must be covered on every shift, not merely on average. A control room strong by day but thin overnight is a real exposure the matrix should surface.

WHY IT MATTERS NOW

One gap is *all it takes*

Security fails at its weakest point, not its average. A single under-covered function, the slow incident response, the lapsed licence, the cyber blind spot, is the gap an incident exploits. A skills matrix is how a manager finds and closes that gap before an adversary does.

8%

GARTNER, 2024

of organisations have reliable workforce skills data, so most security teams judge readiness by impression.

Converged

INDUSTRY GUIDANCE

physical and cyber security is now urged for critical infrastructure, widening the skills a team must hold.

63%

WEF, 2025

of employers call skills gaps the biggest barrier to change; in security they read as functions left exposed.

Security work is unforgiving of hidden gaps: the cost of a thin function is not inefficiency but a breach, an incident mishandled, an intrusion missed, a threat that the team simply was not equipped to counter. And the demands keep widening, as physical and digital security converge, a guarding-only view of capability leaves the cyber-aware, control-room and response skills a modern operation needs unmeasured and unmanaged. A skills matrix

counters this by making **readiness visible across every function**: where cover is genuinely strong, where it is stretched, where a licence is lapsing, where a shift is uncovered. Seeing this lets a security manager target training and recruitment at the weakest links, keep licences current, ensure every critical function is staffed around the clock, and demonstrate to the business that protection rests on measured capability rather than on assumption, before an incident tests the chain at its weakest point.

WHAT IT PROTECTS

Four things a security matrix safeguards

In a security operation, a skills matrix protects four things that bear directly on whether the team can actually keep people and assets safe. Each follows from reading readiness function by function.

PROTECTS 01

The weakest function

By scoring every function, the matrix surfaces the thinnest one, the link an incident would exploit, so it can be strengthened before it is tested.

PROTECTS 02

Round-the-clock cover

It checks each critical function is staffed on every shift, so an operation strong by day is not dangerously exposed overnight.

PROTECTS 03

Licence currency

It tracks the licences and refreshers guarding and CCTV roles require, so no one works a regulated role on a lapsed qualification.

PROTECTS 04

Readiness for converged threats

It maps the widened skill set, including cyber awareness, so the team keeps pace as physical and digital threats merge.

The common thread is **protection you can verify**. A security operation cannot afford to assume it is ready; it must know which functions are strong and which are thin, around the clock, and act on the weak links before they are found the hard way. Capability here is spread across converging physical and digital functions, constrained by licensing, and stretched across every shift. The matrix makes that whole picture visible, so a manager can shore up the weakest link, keep cover continuous and licensed, and meet a widening threat with measured, managed readiness.

THE SCALE BEHIND THE SCORES

The 0 to 5 capability framework

A security matrix needs a scale that distinguishes someone in training from someone who can be trusted to handle an incident alone, and marks the experts who lead and train. This framework, developed by Dr Alex J. Martin-Smith, does that, with Level 3, handles the function unsupervised, as the bar for counting as genuine cover.

0

Not required for the role EXCLUDED

The function is not part of this role. Excluded from the score, keeping the matrix focused on the functions each officer is expected to cover.

1

In training WEIGHTING 25%

Learning the function under supervision. Up to 75% trained. Useful support, but not yet someone to rely on alone for the function in a real incident.

2

Developing WEIGHTING 50%

More than 75% trained; handles routine duties alone, but a serious or unusual incident still needs a more experienced hand. Developing cover.

3

Capable WEIGHTING 75% · COUNTS AS COVER

Handles the function unsupervised to standard, including under pressure. The level that counts as genuine cover for a security function on a shift.

4

Expert / Supervisor WEIGHTING 100%

Deep capability; leads incidents, supervises and trains others. The control room supervisors and senior responders a function depends on, and who develop the team.

5

Strategic ownership / Lead WEIGHTING 100%

Owns the function's standards, procedures and threat response. The security manager or head accountable for how the capability is maintained across the operation.

Read each function as a readiness dial

For each security function, count the people at Level 3 or above with current licences, that is your real, ready cover, and express it as a readiness level for the function. A function sitting low is the **weak link**: under-covered, and the gap an incident would find. Track it per shift too, so a function strong overall but thin overnight is not missed. The aim is for every critical function to read as ready, not just the team as a whole, because security fails at its weakest point.

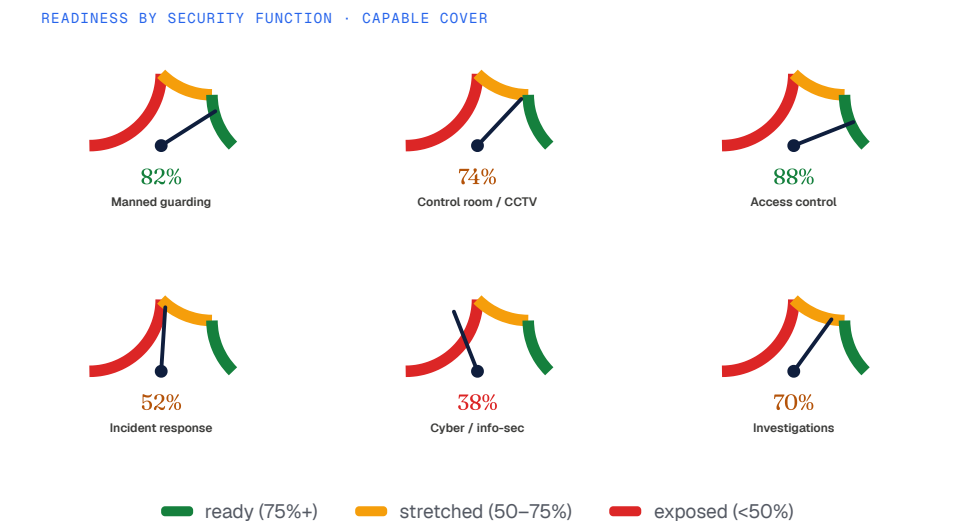
A worked example. Same team, very different function readiness:

```
Access control  readiness 88%  →  strong, well covered
Incident response  52% · cyber awareness 38%  →  the weak
links
the team looks fine on average — the dials show where it is
exposed.
```

SEE THE READINESS

Every function, *on its own dial*

Here is the operation's readiness shown as a cluster of dials, one per security function, each needle pointing to how well that function is covered. A needle in the green is a function ready for what it faces; one in the amber or red is a weak link, stretched or exposed. Reading the dials side by side shows instantly where the chain is strong and where an incident would find its gap.



Cyber & response

are the weak links: incident response and cyber awareness sit lowest, the functions a converged threat would exploit first

Illustrative operation on the Upleashed 0 to 5 framework. Each dial is a security function's readiness from capable, licensed cover; the needle shows the level.

WHAT THE SECURITY MANAGER READS HERE

- **Cyber awareness is the weakest.** The lowest needle, deep in the red. As physical and digital threats converge, this is the gap most likely to be exploited, the priority for training across the whole team, not just specialists.
- **Incident response is stretched.** In the red-amber zone, too thin for an operation that must handle serious events well. Building more capable responders and supervisors here strengthens the most consequential function.
- **Guarding and access control are strong.** Needles in the green, the traditional core is well covered. The risk is complacency: a strong front door does not compensate for a weak response or cyber posture.
- **Read the cluster, not the average.** Averaged together the team looks adequate, but security fails at its weakest function. The dials force attention onto the two that are genuinely exposed.

READY-TO-USE EXAMPLES

Example functions to map for security

A security matrix should map the team against the functions a layered, modern operation depends on, physical and digital alike. Here are ready-

to-adapt categories, a starting point to tailor to your operation.

Category	Examples to map (the columns)	Watch out for
Guarding & patrol	Manned guarding, patrol, search, conflict management, customer-facing	Strong guarding masking weak response or cyber cover
Control room	CCTV monitoring, alarm handling, radio, system operation, logging	Day cover strong but overnight control room thin
Access & systems	Access control, visitor management, biometrics, integrated systems	Reliance on one person who knows the integrated systems
Response & investigation	Incident and emergency response, first aid, investigations, reporting	A thin, under-trained response function for serious events
Cyber & compliance	Cyber and information-security awareness, data handling, licensing	Treating cyber as IT's problem, not a security skill

Map the functions your operation depends on, scored so Level 3 means someone handles the function unsupervised, and read readiness function by function rather than as a single team total. Track licences and refreshers alongside the skill, and check cover on every shift, not just on average. As always, map what matters most, keep the matrix current, and focus development and recruitment on the weakest links the dials reveal.

AVOID THESE

Six mistakes on a security matrix

MISTAKE 01

Judging by the average

A healthy team total hides a weak function. Read readiness function by function.

MISTAKE 02

Guarding-only thinking

The skill set has widened. Map control room, response and cyber, not just guarding.

MISTAKE 03

Ignoring the night shift

Cover that is fine by day can be thin overnight. Check every critical function per shift.

MISTAKE 04

Skill without licence

A lapsed licence is no cover for a regulated role. Track currency, not just the underlying skill.

MISTAKE 05

Cyber as someone else's job

Converged threats need aware officers. Map cyber and information-security awareness as a security skill.

MISTAKE 06

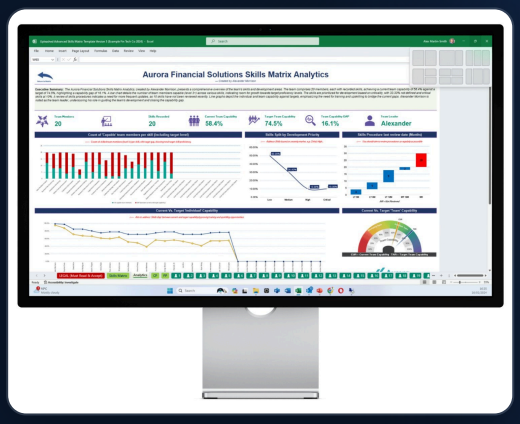
Spreading training evenly

Even effort ignores the weak link. Focus development on the functions the dials show exposed.

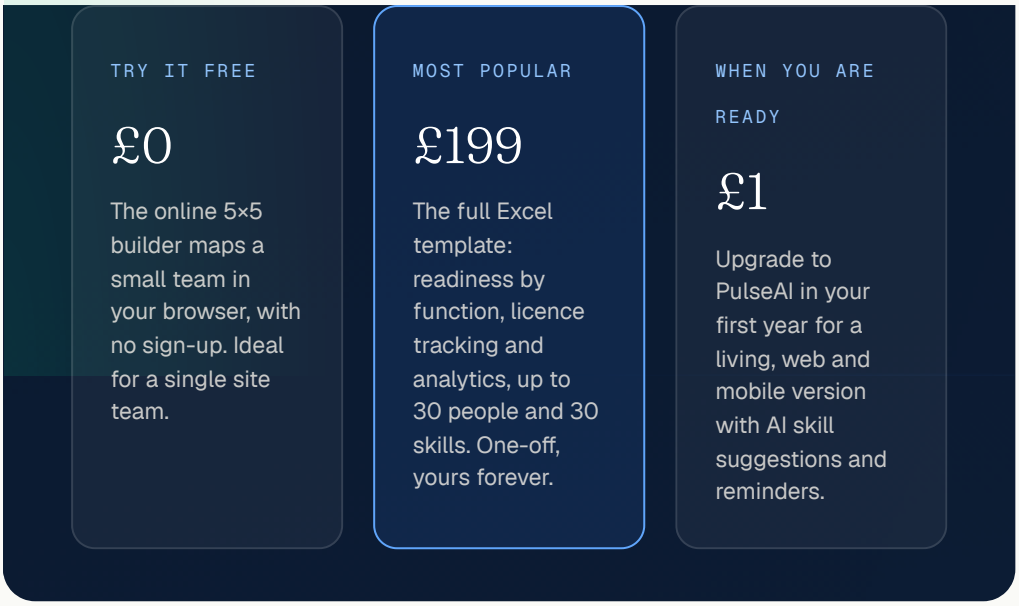
FROM ASSUMED SAFE TO VERIFIED READY

The method is free. A ready-made matrix just makes the weak link *impossible to miss.*

Everything here works in a blank spreadsheet, and that is a fine place to start. A purpose-built template just makes the security view effortless: score the team on the 0 to 5 scale across every function, track licences, and the readiness per function is laid out for you, so the weakest link, the lapsing licences and the uncovered shifts stand out, letting you strengthen the chain before an incident tests it, all on a tool you control.



The Advanced Excel Skills Matrix reads out readiness function by function and tracks licence currency, the basis for strengthening the weakest link and keeping cover continuous, all on the same 0 to 5 framework used throughout this guide.



COMMON QUESTIONS

Quick *answers*

Q What is a skills matrix for a security team?

It is a grid mapping the team against the functions a modern operation depends on, guarding, control room and CCTV, access control, incident response, investigations, and cyber awareness, with a level in each cell. Read function by function, it shows which are ready, which are stretched, and where licensing or shift cover is thin.

Q Why read readiness function by function?

Because security fails at its weakest point, not its average. A team can look well-staffed overall while one critical function, say incident response or cyber awareness, sits dangerously thin. Reading each function separately surfaces that weak link, which is exactly the gap an incident is most likely to exploit.

Q Should a security matrix include cyber skills?

Increasingly, yes. Physical and digital security are converging, and even front-line officers are expected to recognise digital threats. A guarding-only view leaves the cyber-awareness and information-security skills a modern operation needs unmeasured. Mapping them as security skills keeps the team's capability aligned with the threats it actually faces.

Q How does it handle licensing?

By tracking currency, not just the underlying skill. Many guarding and CCTV roles require valid licences and periodic refreshers, and a lapsed licence means a person cannot lawfully cover that role however skilled they are. The matrix records when licences are due so no one is rostered onto a regulated function on an expired qualification.

Q How does it help a 24/7 operation?

By checking cover on every shift, not just on average. A control room or response function that is strong during the day can be dangerously thin overnight. Reading the matrix against the shift pattern reveals where a critical function lacks capable, licensed cover at particular times, so the rota can be balanced before a gap is exposed.

Q Does this work for in-house and contract security alike?

Yes. Whether the team is in-house, outsourced, or a mix, the same approach applies: map the functions the operation depends on, score readiness, track licences, and check cover across shifts. For contracted services it also gives a clear, evidenced basis for assuring that the provider's team genuinely covers every critical function.

ABOUT THE AUTHOR

Dr Alex J. Martin-Smith

CMGR · MBA · LLM · DBA

Alex is the creator of the Upleashed capability framework that powers Skills Matrix Template, the award-winning Excel skills matrix. A Chartered Manager with an MBA, an LLM and a doctorate in business administration, he has spent more than two decades helping operations, HR and quality teams turn capability from a gut feel into something they can measure, manage and prove.

Connect on LinkedIn: linkedin.com/in/alexmartinsmith

Dr Alex J. Martin-Smith

SOURCES

Gartner. (2024). *Talent management research: Workforce skills data.* Gartner.

Martin-Smith, A. J. (n.d.). *The 0 to 5 capability framework.* Upleashed Limited. https://upleashed.com/capability-framework/

Security Industry Association. (n.d.). *Security cornerstones: Physical and cyber convergence.* SIA.

World Economic Forum. (2025). *The future of jobs report 2025.* World Economic Forum.

Strengthen the *weakest link.*

You now have the security method. The quickest way to start is to list your functions, score capable, licensed cover for each, and read them as dials. The needles in the amber and red, and any function thin overnight, are exactly where to focus training and recruitment before an incident finds the gap.