MOORE eSSENTIALS

THE SEARCH FIRM SECURITY AUDIT

10 categories. 60 questions. One rule: "I don't know" counts as no.

Tricia Tamkin | Moore eSSentials | 2026

You've heard me say it for decades. My first job is to protect you. My second job is to make you money. This audit is the first job. Work through all ten categories and answer honestly. Each question takes seconds. The whole thing takes an afternoon. When you're done, you'll know exactly where your firm is exposed and what to fix first.

HOW TO SCORE IT

Three answers are allowed: Yes, No, and Don't Know. Don't Know counts as No, because attackers don't care whether your exposure is deliberate or accidental. If a question confuses you, the confusion itself is a finding. Write it down and ask whoever runs that system.

Eight questions are marked **RED FLAG**. A No on any of them gets fixed this week, before anything else. Everything else gets fixed in category order. The categories are sequenced by where search firms actually lose money, so start at the top and work down.

Nothing here requires an IT department. Most fixes are settings, habits, and short conversations. A handful cost money. All of them cost less than one rerouted placement fee.

01 EMAIL

Email is where search firms actually get robbed. Not by genius hackers. By someone reading your inbox for three weeks and then sending one well-timed message.

QUESTION	YES	NO	DON'T KNOW
RED FLAG. Does every email account at the firm require multi-factor authentication, with no exceptions for the owner?	☐	☐	☐
Is every email password unique and stored in a password manager instead of a browser, a spreadsheet, or a notebook?	☐	☐	☐
Have you checked every inbox in the last 90 days for forwarding rules or delegate access nobody remembers creating?	☐	☐	☐
Are SPF, DKIM, and DMARC configured on your sending domain? Ask whoever runs your email. A blank stare counts as No. Bonus: these also improve your outreach deliverability.	☐	☐	☐
Would your team catch a lookalike domain, one letter off from a client's real one, in the middle of a busy reply chain?	☐	☐	☐
Could you lock down a compromised mailbox within an hour, including on a Saturday?	☐	☐	☐

02 MONEY MOVEMENT

Placement fees are big, irregular, one-time wires. That's the exact profile fraudsters hunt, because nobody expects the invoice twice.

QUESTION	YES	NO	DON'T KNOW
RED FLAG. Is every change to banking or payment details verified by a phone call to a number you already had on file, never a number from the email requesting the change?	☐	☐	☐
Does a second person approve every outbound wire and	☐	☐	☐

QUESTION	YES	NO	DON'T KNOW
every change to where client payments land?			
Have you told clients in writing how you'll always invoice, and that banking changes will never arrive by email alone?	☐	☐	☐
Do you reconcile expected fees against received payments fast enough to catch a rerouted invoice within days instead of at quarter end?	☐	☐	☐
Does everyone who touches invoicing know what business email compromise looks like?	☐	☐	☐
Do you know exactly who to call at your bank the moment a wire goes sideways, and how few hours you have to claw it back?	☐	☐	☐

03 IDENTITY AND ACCESS

Every tool you use is a door. This category counts the doors and asks who's holding keys.

QUESTION	YES	NO	DON'T KNOW
RED FLAG. Does the whole firm use a password manager, with zero passwords reused across tools?	☐	☐	☐
Is multi-factor authentication turned on for the ATS, LinkedIn, job boards, and banking, using an authenticator app instead of text messages wherever possible?	☐	☐	☐
Are shared logins eliminated, or at minimum documented so you can name every person holding each one?	☐	☐	☐
RED FLAG. When someone leaves (employee, splits partner, contractor), does a same-day checklist kill every credential they ever touched?	☐	☐	☐
Can you say with certainty that nobody who's left the firm still has working access? Don't Know counts as No, and it usually is.	☐	☐	☐

QUESTION	YES	NO	DON'T KNOW
Is daily work done in standard accounts, with admin rights reserved for the moments they're actually needed?	☐	☐	☐

04 THE HUMAN LAYER

Your people open attachments from strangers for a living. Training them is now part of the job description.

QUESTION	YES	NO	DON'T KNOW
Has everyone at the firm had at least one hour of training this year on phishing, fake candidates, and voice cloning?	☐	☐	☐
Are resumes opened in a preview pane or protected view first, and does everyone know the file types you never open: .exe, .scr, .html attachments, macro-enabled documents?	☐	☐	☐
Is there a verification step before submittal: live video with natural movement, references called at independently found numbers, identity checks for remote hires?	☐	☐	☐
Would your team recognize the classic tells of a deepfaked video interview, and is there a fallback verification when the tells fail?	☐	☐	☐
Is there a callback rule or code word for unusual requests arriving by phone from “clients” or “teammates”?	☐	☐	☐
Is there a no-blame rule so whoever clicked the bad link reports it in minutes instead of hiding it for days?	☐	☐	☐

05 CANDIDATE AND CLIENT DATA

A hacker sees your firm as a database with weak locks. Comp data, addresses, sometimes SSNs, and every fee agreement you've ever signed.

QUESTION	YES	NO	DON'T KNOW
Can you list exactly what personal data the firm holds and every place copies live: the ATS, spreadsheets, inboxes, download folders?	☐	☐	☐
Are export and bulk-download rights limited and logged, so one departing recruiter can't walk out with the whole database?	☐	☐	☐
Do you delete or archive candidate data you no longer need instead of keeping everything forever?	☐	☐	☐
Do you know which state privacy and breach-notification laws apply to the candidates in your database?	☐	☐	☐
Do your client agreements spell out your data-protection obligations, and could you meet them today?	☐	☐	☐
Is the most sensitive data, especially SSNs, encrypted or restricted beyond a shared drive everyone can open?	☐	☐	☐

06 AI TOOLS

AI is the newest door, and most firms never wrote down the rules. These questions write them down.

QUESTION	YES	NO	DON'T KNOW
RED FLAG. Does the firm have a written AI policy naming the approved tools and the data that never gets pasted into any of them?	☐	☐	☐
Is candidate and client data only ever entered into paid or enterprise AI tiers with training on your data turned off?	☐	☐	☐
Can you name every AI tool with live access to email,	☐	☐	☐

QUESTION	YES	NO	DON'T KNOW
calendars, or browsing, and what it could do if hijacked?			
Do you know where every AI notetaker transcript from client and candidate calls is stored, and who can read it?	☐	☐	☐
If AI writes code or automations for the firm, does a human review the output before it touches real systems or data?	☐	☐	☐
If you screen resumes with AI, do you know applicants and attackers hide invisible instructions inside documents to manipulate the tools reading them?	☐	☐	☐

07 VENDORS AND CONTRACTORS

The offshore sourcer, the VA, the web developer from 2021. Access accumulates quietly until somebody hostile finds it.

QUESTION	YES	NO	DON'T KNOW
RED FLAG. Can you produce a complete list of every outside party with access to your systems: sourcers, VAs, developers, IT support, marketing help?	☐	☐	☐
Does each contractor have only the access their job requires instead of full run of the ATS and the inbox?	☐	☐	☐
Has every contractor's access been reviewed in the last six months?	☐	☐	☐
Is contractor offboarding as rigorous as employee offboarding, with credentials killed the day the engagement ends?	☐	☐	☐
Have you reviewed which third-party apps hold standing access to your email or drive, and revoked the ones you forgot you approved?	☐	☐	☐
Do contracts with anyone touching your data include confidentiality and security obligations?	☐	☐	☐

08 DEVICES AND NETWORKS

The fanciest security in the world dies on an unpatched laptop riding hotel wifi.

QUESTION	YES	NO	DON'T KNOW
Is full-disk encryption turned on for every laptop that touches firm data?	☐	☐	☐
Are operating systems and browsers set to update automatically, and do the machines actually get restarted?	☐	☐	☐
Has every home office router had its default password changed and its firmware updated within the last year?	☐	☐	☐
Does everyone use a VPN or a phone hotspot on public wifi instead of trusting the hotel network with candidate data?	☐	☐	☐
Do personal phones carrying work email have a screen lock and the ability to be wiped remotely?	☐	☐	☐
Is real endpoint protection running on every machine, beyond whatever shipped with it?	☐	☐	☐

09 BACKUPS AND CONTINUITY

Ransomware doesn't negotiate with firms that have backups. This category decides which kind of firm you are.

QUESTION	YES	NO	DON'T KNOW
RED FLAG. Is the ATS and other critical data backed up on a schedule to somewhere ransomware can't reach: offline, or a separate account with different credentials?	☐	☐	☐
Have you ever actually tested a restore, or is the backup a matter of faith?	☐	☐	☐
Could the firm run for a week with email and the ATS down, and is that plan written anywhere?	☐	☐	☐
If LinkedIn locked or lost your account tomorrow, do you have	☐	☐	☐

QUESTION	YES	NO	DON'T KNOW
exported connections, secondary admins on the company page, and another way to reach your network?			
Do fee agreements and contracts exist somewhere beyond the one system that currently holds them?	☐	☐	☐
Do you know how long your key tools keep your data if an account is closed, hijacked, or the vendor folds?	☐	☐	☐

10 INCIDENT RESPONSE

Bad days come. The plan you wrote calmly beats every decision you'll make in a panic.

QUESTION	YES	NO	DON'T KNOW
RED FLAG. Does a one-page plan exist on paper naming who gets called, in what order, when something breaks: IT, bank, insurer, lawyer, clients?	☐	☐	☐
Do you carry cyber insurance, know what it excludes, and actually have the controls (like MFA) the application says you have?	☐	☐	☐
Do you know your legal notification obligations if candidate data leaks?	☐	☐	☐
Has the firm ever run a 30-minute tabletop exercise: “we just lost email, go”?	☐	☐	☐
Does everyone know the first moves that preserve evidence: disconnect the machine, don't wipe it, don't quietly pay?	☐	☐	☐
Is there a communication plan for telling clients bad news before they hear it somewhere else?	☐	☐	☐

THE RED FLAG EIGHT

If you fix nothing else this month, fix these. Every one is a same-week job.

1. Multi-factor authentication on every email account, no exceptions.
2. Payment changes verified by phone to a number already on file.
3. A password manager for the whole firm, zero reuse.
4. Same-day credential kill when anyone leaves.
5. A written AI policy naming tools and forbidden data.
6. A complete list of every outsider with system access.
7. Backups a ransomware attack can't reach.
8. A one-page incident plan that exists on paper.

WHAT NOW

Count your No and Don't Know answers by category. Fix the red flags this week. Then work the categories top to bottom, one per week if you need a pace. Reruns matter more than perfection: put a calendar reminder in for six months from now and take the audit again.

This audit is free, ungated, and yours to share with any firm owner who needs it. That's the whole deal. Consider it a Random Act of Kindness for our industry, because the industry's been good to me. If you're in recruiting and want more free, high-value content, you know where to find us.

mooreessentials.com