inforcer

The MSP QBR Checklist

How to prove your value and win new business in every Quarterly Business Review

Tick each point off as you prepare and present. The goal of every QBR is to make your value understandable to the people who pay for it, close the loop between the threats you've stopped and the policies that prevent them, and open the next conversation – renewal, upsell, or new business.

1 Before the QBR: build your evidence

Walk in with proof, not promises.

- [ ] **Pull a customer focused report** for the quarter. This is your documented record of all actions taken and improvements made during the period.
- [ ] **Pull usage and adoption data:** assess Microsoft 365 license utilization, active users, and feature adoption since your last review.
- [ ] **Review every threat detected and contained** since your last review, and pick out the headline wins worth walking through.
- [ ] **List the tenant management delivered** this quarter: policy configuration, drift monitoring, and ongoing hardening – and the value this brings your customer.
- [ ] **Assess key AI metrics:** monitor Copilot or AI usage, any unmanaged "shadow" AI tools in play, and Copilot licenses paid for but sitting unused.
- [ ] **Spot upsell opportunities:** note the gaps between what the customer has today and the protection, productivity, and posture you would recommend.
- [ ] **Know your room.** Confirm who's attending and what they care about. Remember owners and directors think in productivity, profitability, and risk, not policies.
- [ ] **Strip the jargon.** Translate your technical work into plain English before you present it.

2 Business priorities: lead with what the customer cares about

Stakeholders care about efficiency, productivity, revenue, and growth, rather than technical details. Keep information results focused to keep customers engaged.

- [ ] **Review customer objectives for the quarter ahead:** e.g. growth, productivity, efficiency, compliance, cost control and map these to their IT.
- [ ] **Frame security as business outcomes:** protected revenue, uptime, continuity, and reduced risk, not policy updates and fixes.
- [ ] **Connect your work to their productivity.** Show how what you do keeps their people working effectively and without disruption.
- [ ] **Quantify the value** in numbers a board would follow: threats contained, incidents prevented, downtime avoided.
- [ ] **Report at boardroom level.** Make it an update the decision maker could repeat to their peers, not a log file only your team understands.
- [ ] **Reinforce trust.** Map out how you make your service personal and reliable: e.g. regular contact, clear ownership, and consistent availability to make them feel like a priority.

3 Cyber security: show the full picture

Combine prevention and detection for a unified service. Siloing security no longer makes sense.

- [ ] **Lead with the right-of-boom wins:** the threats you detected and contained this quarter – the visible, easy-to-quantify work.
- [ ] **Show a real-time threat map** with threat volume, origins, and patterns to make the risk real. Filter per threat type if necessary.
- [ ] **Tell the story in plain English.** Walk through key incidents as attack narratives: what happened, who was affected, and what you did about it.
- [ ] **Map each significant threat to a policy.** Identify the exact Microsoft 365 configuration that would stop it recurring.
- [ ] **Evidence your left-of-boom work:** Microsoft 365 policy configuration, drift monitoring, and continual tenant hardening.
- [ ] **Be straight about risk.** No tenant is 100% secure, which is exactly why prevention and detection have to work together.
- [ ] **Make the invisible visible** contrast the disruption they didn't experience with what a breach would have cost them.

4 Productivity and adoption: getting the most from Microsoft 365

Unlocking the enterprise-grade productivity and security contained in your customers' Microsoft 365 licensing.

- [ ] **Review license utilization.** Assess active users versus licenses paid for and flag anything bought but going unused.
- [ ] **Surface underused tools.** Highlight adoption of what they already own and where uptake is low.
- [ ] **Clear the productivity blockers.** Pull the recurring issues from the ticket trend (slow sign-ins, sync problems etc.) and show how you've resolved them.
- [ ] **Recommend enablement:** targeted training or configuration that turns underused licenses into real, everyday productivity.
- [ ] **Tie adoption to their goals** connect specific Microsoft 365 applications and capabilities to the business outcomes the customer actually cares about, such as enhanced collaboration and increased efficiency.

5 AI readiness and enablement: help them adopt AI safely

Tenant security is the foundation of any successful AI initiative.

- [ ] **Assess AI readiness.** Secure the Microsoft 365 tenant, ensure proper governance, and assess access control before Microsoft 365 Copilot is switched on.
- [ ] **Surface oversharing risk.** AI exposes whatever a user can already reach. Tighten permissions and sensitivity labels before rollout.
- [ ] **Find the shadow AI** identify unmanaged AI tools staff are already using, and the data risk that comes with them.
- [ ] **Set the guardrails** agree the policies, access controls, and usage guidance that let them adopt AI with confidence.
- [ ] **Highlight Microsoft 365 power users** who will see the most benefit from their Copilot licenses.
- [ ] **Identify use cases for AI.** Highlight departments or areas of the business which will see the most ROI from AI, and create business cases and enablement sessions.

6 Licensing, cost and IT operations: run a tight, efficient estate

Efficiency is value the customer can see on the invoice.

- [ ] **Right-size licenses:** remove duplicate, unused, or over-specified licenses and put a number on the saving.
- [ ] **Report service health:** uptime, ticket volumes, and response and resolution times across the quarter.
- [ ] **Confirm resilience:** ensure backup, recovery, and business continuity strategies are in place and have been tested, not just assumed.
- [ ] **Stay current.** Keep devices and the tenant patched and up to date against the latest Microsoft changes.
- [ ] **Map the roadmap.** Unpack the Microsoft updates and projects coming next quarter, and what they mean for the business.

7 Win new business and upsell

Look to the future: every QBR is an opportunity to win new business – for you and your customer.

- [ ] **Close the loop, threat to policy.** Take a contained threat and show the exact policies that would have prevented it.
- [ ] **Recommend the next services:** continuous tenant management, monitoring, and hardening, tied directly to the risks you've just shown.
- [ ] **Upsell productivity and adoption:** managed enablement, training, or configuration that unlocks the licenses they already pay for.
- [ ] **Upsell AI enablement initiatives** to help customers get the most out of their AI tools.

8 After the QBR: close the loop

The review isn't finished until the next step is booked.

- [ ] **Send the plain-English summary:** a short recap of the value delivered and the next steps agreed.
- [ ] **Log it in your PSA.** Feed incidents and actions into your PSA to cut noise and keep everything in one place.
- [ ] **Confirm what was agreed.** Capture the upsell or policy changes with clear owners and dates.
- [ ] **Book the next touchpoint.** Schedule the next check-in or QBR so the customer always knows where they stand.

Want to make showing your value easier than ever?

inforcer TDR has advanced reporting capabilities, that allow you to demonstrate clear attack narratives in plain English and upsell the value of preventative tenant management. See how inforcer could make showing your value easier than ever and take your QBRs to the next level.

Download a sample report

inforcer