6 Steps for Assuring Microsoft 365 Security:

Through Technology

Trust Cloud Security

Microsoft provide evidence of their system and process security on Trust Centre. Also consider the benefits of SaaS over bespoke on-premise solutions:

- Massive investment in security innovation
- Greater Threat Intelligence from all customers
- Better automation and anomaly detection
- Common controls across multiple applications
- Openness
- Standardisation & shared knowledge

Assure Technical Solution

"Software as a Service is not a managed Service"

It is the ***customer's responsibility*** to ensure the correct configuration of SaaS, hybrid services and migration tooling. Follow appropriate guidance and best practice. Have an experienced team assure your supplier's design, configuration and processes or undertake a Red Team Review of your own team's work.

Manage Change

Microsoft ***will*** change the Office 365 platform during your transition. You need processes in place to review the changes that Microsoft post on their roadmap, blogs and Message Centre from the start of your transition and forever after.

Microsoft launch features in Office 365 configured for maximum adoption, this may not match your organisation's requirements or security posture.

Evidence Component Security

The old model of per-service IT Health Checks isn't well suited to SaaS and Hybrid solutions.

Significant security assurance comes from standard delivery processes, including build checks, component, integration and user testing, patching reports, service processes etc.

Build "evidence packs" of these showing correct implementation and operation.

Test End to End

Test security end to end (ideally with specialist resources) with scenarios based upon the principal risks to your organisation.

These scenarios must be end-to-end, including end user device configuration.

This should result in an IT Health Check response with a number of remediation activities for you or your supplier to undertake.

Ongoing Security Assurance

Monitor your tenant through Microsoft's security and compliance tools and/or integration with your own SIEM solution. Set up effective security management processes using Microsoft Tooling.

Undertake periodic red team reviews of your configuration and processes. Test your own security with simulated breaches and continue to update your user education to reflect new products and new threats.