



CIS MICROSOFT 365 FOUNDATIONS BENCHMARK EVIDENCE

Fabrikam Dental Group

PREPARED BY

Harbour IT

DATE

12 October 2026

EVIDENCE DATE

12 Oct 2026

SCHEME

Center for Internet Security

MICROSOFT 365 TENANT

fabrikam.onmicrosoft.com

● Gaps to close

Fabrikam Dental Group has 9 controls not in place.

IN THIS REPORT

Summary	2
Gaps to close	3
Microsoft 365 admin centre	5
Microsoft Entra ID	7
Exchange Online	12
SharePoint, OneDrive and Teams	15
Intune and devices	17
About this evidence	19

Summary

Fabrikam Dental Group has 9 controls not in place.

The benchmark's recommendations that Office Sentry reads, judged setting by setting, with the fix for each. Use it as the evidence for a CIS-aligned audit or a client's hardening baseline.

32 controls



Gaps to close

The controls most likely to be queried, with the fix for each.

1 No guests or apps with admin roles

1 guest with admin roles. Fix: Remove admin roles from guest accounts.

2 MFA required for administrative roles

1 admin not covered by MFA. Fix: Have each listed admin register a strong method.

3 Legacy authentication blocked

Legacy authentication is allowed. Fix: Block legacy authentication.

4 Users can't consent to apps

Users can consent to any app. Fix: Set user consent to "Allow user consent for apps from verified publishers, for selected permissions" or turn it off and use the admin consent workflow.

5 Users can't register applications

Any user can register an app. Fix: Set "Users can register applications" to No.

6 No inbox rules hiding mail

1 suspicious inbox rule. Fix: Check each rule with the mailbox owner.

7 SMTP AUTH disabled

SMTP AUTH is on for the organisation. Fix: Turn off SMTP AUTH for the organisation and enable it only on the mailboxes of devices or apps that still need it.

8 Disks encrypted

6 of 54 computers not encrypted. Fix: Turn on BitLocker.

9 Supported operating systems

7 of 54 Windows computers past end of support. Fix: Upgrade computers on Windows 10 or an old Windows 11 release to the current Windows 11 release.

10 MFA required for all users

Enforced by CA002 — All users: Require MFA, with 1 exclusion to review. Fix: Create a Conditional Access policy requiring MFA for all users and all cloud apps, or turn on Security Defaults if the tenant has no Entra ID P1.

11 Phishing-resistant MFA for administrators

2 admins without a phishing-resistant method. Fix: Have each listed admin register a passkey.

12 Weak authentication methods not relied on

4 people can only use a text or call as a second factor. Fix: Ask these people to set up the Microsoft Authenticator app.

13 Guest access to the directory restricted

Anyone, including guests, can invite guests. Fix: Restrict guest invitations to admins and the Guest Inviter role, or at least to members, under External collaboration settings.

14 All forms of mail forwarding blocked

5 external forwards. Fix: Remove forwarding to outside addresses unless the client has a documented business reason.

15 SPF records published

1 domain with SPF problems. Fix: Publish one SPF record per domain ending in -all.

16 DKIM enabled

1 mail domain without DKIM. Fix: Turn on DKIM for each domain in the Defender portal.

17 DMARC published and enforced

2 domains without DMARC enforcement. Fix: Publish a DMARC record with a rua= reporting address, start at p=none to see who sends as the domain, then move to p=quarantine and p=reject.

18 External sharing restricted

Anyone, including anonymous links. Fix: Change SharePoint external sharing to "New and existing guests".

19 No anyone links in use

2 files and folders shared with anyone. Fix: Remove anyone links that are no longer needed, and set the rest to view-only with an expiry date.

20 Every group and team has an owner

4 teams and groups without an owner. Fix: Make an active person, ideally two, an owner of each listed team or group.

21 Devices enrolled and compliant

1 of 55 joined computers not in Intune. Fix: Enrol Entra-joined and hybrid-joined computers in Intune.

Microsoft 365 admin centre

● Fail

Few, cloud-only Global Administrators, no shared mailboxes anyone can sign in to, and a way to get apps approved.

Two to four Global Administrators

● Pass

Between two and four accounts hold the Global Administrator role.

WHAT WE FOUND

- 2 Global Administrators.
- Accounts holding privileged roles: 4
- Admins with no MFA policy: 1
- Admins with no MFA method registered: 2

What Microsoft 365 can't show: Judged from Entra ID role assignments, including through groups.

Administrative accounts are cloud-only

● Pass

Accounts with admin roles aren't synchronised from on-premises Active Directory.

WHAT WE FOUND

- Cloud-only tenant: no accounts are synced from on-premises AD.

What Microsoft 365 can't show: Judged from Entra ID admin role holders.

Sign-in to shared mailboxes is blocked

● Pass

The accounts behind shared mailboxes can't be signed in to.

WHAT WE FOUND

- All 3 shared mailboxes block sign-in.

What Microsoft 365 can't show: Judged from Exchange Online and Entra ID.

No guests or apps with admin roles

 Fail

Admin roles are held by internal people, not guests, and apps holding roles are reviewed.

GAPS

- 1 guest with admin roles.
 - g#EXT#@fabrikam.example: Guest holding Exchange Administrator
- 1 app with privileged roles.
 - Some app: App holding Exchange Administrator

Fix: Remove admin roles from guest accounts. If an external partner needs access, use GDAP or a member account in this tenant protected by MFA.

Text to paste: 1 guest with admin roles. 1 app with privileged roles.

What Microsoft 365 can't show: Judged from Entra ID role assignments.

Microsoft Entra ID

● Fail

MFA for everyone with Conditional Access, phishing-resistant MFA for admins, legacy authentication blocked, no user consent to apps, and users can't register apps, create tenants or join by email.

MFA required for all users

● Partly

A Conditional Access policy requires multi-factor authentication for every user.

WHAT WE FOUND

- But: 27 users without MFA.
- Users with an MFA method registered: 50.9% of 55
- Accounts covered by an enforced MFA policy: 54 of 55
- Not covered: breakglass@fabrikam.example

GAPS

- Enforced by CA002 — All users: Require MFA, with 1 exclusion to review.
 - breakglass@fabrikam.example: Excluded from "CA002 — All users: Require MFA"

Fix: Create a Conditional Access policy requiring MFA for all users and all cloud apps, or turn on Security Defaults if the tenant has no Entra ID P1. Keep exclusions to break-glass accounts.

Text to paste: Enforced by CA002 — All users: Require MFA, with 1 exclusion to review.

What Microsoft 365 can't show: Judged from Conditional Access and Security Defaults.

MFA required for administrative roles

● Fail

A Conditional Access policy requires multi-factor authentication for every admin role.

WHAT WE FOUND

- Accounts holding privileged roles: 4
- Admins with no MFA policy: 1
- Admins with no MFA method registered: 2

GAPS

- 1 admin not covered by MFA.
 - breakglass@fabrikam.example: Global Administrator: excluded from CA001 — Admins: Require phishing-resistant MFA, CA002 — All users: Require MFA, CA005 — Block sign-ins from disallowed countries, CA006 — Require MFA for Azure management, CA007 — Admins: No persistent browser, 8h sign-in frequency, CA008 — All users: 8h sign-in frequency, CA009 — Require MFA for device registration, CA010 — Insider risk: Step-up MFA, CA011 — High sign-in risk: Block
- 1 admin without MFA, and 1 whose registration isn't known.
 - breakglass@fabrikam.example: Global Administrator with no MFA method registered
 - g#EXT#@fabrikam.example: Exchange Administrator: MFA registration unknown

Fix: Have each listed admin register a strong method (Authenticator or a FIDO2 key), or remove the role. Break-glass accounts should use FIDO2 keys kept offline.

Text to paste: 1 admin not covered by MFA. 1 admin without MFA, and 1 whose registration isn't known.

What Microsoft 365 can't show: Judged from Conditional Access and Entra ID admin roles.

Phishing-resistant MFA for administrators

● Partly

Administrators sign in with a phishing-resistant method (passkey, FIDO2 key or Windows Hello for Business).

GAPS

- 2 admins without a phishing-resistant method.
 - anna.kowalski@fabrikam.example: Global Administrator; signs in with Authenticator app
 - breakglass@fabrikam.example: Global Administrator; signs in with no MFA method at all

Fix: Have each listed admin register a passkey (in Microsoft Authenticator or on a security key) or Windows Hello for Business, then require the Phishing-resistant MFA authentication strength for admin roles in Conditional Access. Codes and push approvals can be relayed by a fake sign-in page; these can't.

Text to paste: 2 admins without a phishing-resistant method.

What Microsoft 365 can't show: Judged from the methods each admin has registered.

Weak authentication methods not relied on

● Partly

Text messages and voice calls aren't anyone's only second factor.

GAPS

- 4 people can only use a text or call as a second factor.
 - george.baker@fabrikam.example: Second factor is only Mobile phone (SMS or call)
 - owen.robinson@fabrikam.example: Second factor is only Mobile phone (SMS or call)
 - owen.turner@fabrikam.example: Second factor is only Mobile phone (SMS or call)
 - thomas.allen@fabrikam.example: Second factor is only Mobile phone (SMS or call)

Fix: Ask these people to set up the Microsoft Authenticator app (the registration campaign in the authentication methods policy prompts them at sign-in), then turn off text message and voice call sign-in, or keep them only as a backup. Texts and calls can be intercepted or moved to an attacker's SIM.

Text to paste: 4 people can only use a text or call as a second factor.

What Microsoft 365 can't show: Judged from Entra ID authentication methods.

Legacy authentication blocked

● Fail

A Conditional Access policy blocks legacy authentication.

GAPS

- Legacy authentication is allowed.
 - No enabled policy blocks legacy authentication for all users

Fix: Block legacy authentication (Exchange ActiveSync and other clients) with a Conditional Access policy for all users. Legacy protocols can't do MFA and are the most common password-spray target.

Text to paste: Legacy authentication is allowed.

What Microsoft 365 can't show: Judged from Conditional Access.

Users can't consent to apps

● Fail

User consent to applications is turned off (or limited to verified publishers and low-risk permissions).

GAPS

- Users can consent to any app.
 - Any user can grant any app access to their mail and files

Fix: Set user consent to "Allow user consent for apps from verified publishers, for selected permissions" or turn it off and use the admin consent workflow. Consent phishing relies on this setting.

Text to paste: Users can consent to any app.

What Microsoft 365 can't show: Judged from Entra ID consent settings.

Admin consent workflow on

● Pass

Users can ask for an app to be approved, and admins review the request.

WHAT WE FOUND

- Users can consent to most apps themselves, so admin consent requests are off (see the user consent check).

What Microsoft 365 can't show: Judged from Entra ID consent settings.

Users can't register applications

● Fail

Only admins can register applications.

GAPS

- Any user can register an app.
 - Users can register apps that nobody reviews

Fix: Set "Users can register applications" to No (Entra admin center > Users > User settings) and give the Application Developer role to the people who need it.

Text to paste: Any user can register an app.

What Microsoft 365 can't show: Judged from Entra ID user settings.

Non-admins can't create tenants

● Not collected

Users who aren't admins can't create new tenants.

WHAT WE FOUND

- Not checked: users can't create new tenants (Microsoft didn't return this setting).

What Microsoft 365 can't show: Judged from Entra ID user settings.

Guest access to the directory restricted

● Partly

Guests have limited access to directory objects, and only admins and the Guest Inviter role can invite.

WHAT WE FOUND

- Guests have limited access to directory objects (the default).

GAPS

- Anyone, including guests, can invite guests.
 - Guests can invite other guests

Fix: Restrict guest invitations to admins and the Guest Inviter role, or at least to members, under External collaboration settings.

Text to paste: Guests have limited access to directory objects (the default). Anyone, including guests, can invite guests.

What Microsoft 365 can't show: Judged from Entra ID external collaboration settings.

No joining the tenant by email verification

● Not collected

People can't join the tenant just by verifying an email address.

WHAT WE FOUND

- Not checked: people can't join the tenant just by verifying an email address (Microsoft didn't return this setting).

What Microsoft 365 can't show: Judged from Entra ID authorisation settings.

Group creation limited

● Pass

Only chosen people can create Microsoft 365 groups and teams.

WHAT WE FOUND

- Only admins and members of Group creators can create teams and groups.

What Microsoft 365 can't show: Judged from Entra ID group settings.

Risky users and sign-ins dealt with

● Not collected

Entra ID Protection risk is acted on: no account left at risk, no risky sign-in left open.

WHAT WE FOUND

- Not checked: no accounts are at risk in Entra ID Protection (Risky users need Entra ID P2).
- Not checked: no risky sign-ins succeeded (Sign-in risk needs Entra ID P2).

What Microsoft 365 can't show: Judged from Entra ID Protection (Entra ID P2 for the full detections).

Password hash sync on (hybrid)

● Not collected

Where accounts sync from Active Directory, password hash sync is on so leaked credentials are detected.

WHAT WE FOUND

- Not checked: password hash sync is on (Cloud-only tenant: directory sync isn't turned on).

What Microsoft 365 can't show: Judged from Entra Connect; not applicable to cloud-only tenants.

Exchange Online

● Fail

Auditing on, no forwarding outside, SMTP AUTH off, and every domain with SPF, DKIM and DMARC.

Mailbox auditing on

● Pass

Mailbox auditing is on for every user mailbox.

WHAT WE FOUND

- Mailbox auditing is on for the organisation.

What Microsoft 365 can't show: Judged from Exchange Online.

All forms of mail forwarding blocked

● Partly

Automatic forwarding to outside addresses is blocked by policy, and no mailbox or rule forwards out.

WHAT WE FOUND

- The default outbound policy blocks automatic external forwarding.

GAPS

- 5 external forwards.
 - anna.kowalski@fabrikam.example: Mailbox forwarding to anna.kowalski@homemail.example (keeps a copy)
 - anna.kowalski@fabrikam.example: Inbox rule "Copy to home" forwards to anna.kowalski.home@homemail.example
 - rhys.hall@fabrikam.example: Mailbox forwarding to rhys.hall@homemail.example (doesn't keep a copy)
 - rhys.walker@fabrikam.example: Mailbox forwarding to rhys.walker@homemail.example (doesn't keep a copy)
 - thomas.robinson@fabrikam.example: Inbox rule "Invoices to bookkeeper" forwards to bookkeeping@ledgerline.example

Fix: Remove forwarding to outside addresses unless the client has a documented business reason. Forwarding is the most common way attackers keep reading a mailbox after a password reset.

Text to paste: The default outbound policy blocks automatic external forwarding. 5 external forwards.

What Microsoft 365 can't show: Judged from the outbound spam policy, mailbox forwarding and inbox rules.

No inbox rules hiding mail

● Fail

Inbox rules that delete, hide or redirect mail are found and reviewed.

GAPS

- 1 suspicious inbox rule.
 - anna.kowalski@fabrikam.example: ".": Moves to RSS Feeds mail mentioning invoice, payment; Rule name '' looks deliberately blank

Fix: Check each rule with the mailbox owner. Rules that delete or bury messages about payments or security alerts are a sign of a compromised account: reset the password, revoke sessions and review sign-ins.

Text to paste: 1 suspicious inbox rule.

What Microsoft 365 can't show: Judged from Exchange Online inbox rules.

SMTP AUTH disabled

● Fail

Authenticated SMTP is turned off for the organisation.

GAPS

- SMTP AUTH is on for the organisation.
 - SMTP AUTH is allowed

Fix: Turn off SMTP AUTH for the organisation and enable it only on the mailboxes of devices or apps that still need it, such as scanners. It accepts passwords without MFA.

Text to paste: SMTP AUTH is on for the organisation.

What Microsoft 365 can't show: Judged from Exchange Online transport settings.

SPF records published

● Partly

Every mail domain publishes an SPF record.

GAPS

- 1 domain with SPF problems.
 - parked.example: Doesn't receive mail but has no "v=spf1 -all" record to stop spoofing

Fix: Publish one SPF record per domain ending in -all (or ~all while testing), e.g. "v=spf1 include:spf.protection.outlook.com -all". Domains that never send mail should publish "v=spf1 -all".

Text to paste: 1 domain with SPF problems.

What Microsoft 365 can't show: Judged from public DNS.

DKIM enabled

● Partly

DKIM signing is on for every mail domain.

GAPS

- 1 mail domain without DKIM.
 - fabrikam.example: Microsoft 365 DKIM isn't set up (selector2 CNAME missing)

Fix: Turn on DKIM for each domain in the Defender portal (Email authentication settings > DKIM), publishing the two selector CNAME records it shows. This applies to domains behind a mail gateway too when Microsoft 365 still sends for them (their SPF includes spf.protection.outlook.com); a gateway signs only the mail that goes out through it.

Text to paste: 1 mail domain without DKIM.

What Microsoft 365 can't show: Judged from Exchange Online and public DNS.

DMARC published and enforced

● Partly

Every domain publishes a DMARC record with a quarantine or reject policy.

GAPS

- 2 domains without DMARC enforcement.
 - fabrikam.example: DMARC is monitor-only (p=none); spoofed mail is still delivered
 - parked.example: Doesn't receive mail but has no DMARC p=reject record

Fix: Publish a DMARC record with a rua= reporting address, start at p=none to see who sends as the domain, then move to p=quarantine and p=reject. Without enforcement, spoofed mail from the domain is delivered.

Text to paste: 2 domains without DMARC enforcement.

What Microsoft 365 can't show: Judged from public DNS.

SharePoint, OneDrive and Teams

● **Partly**

External sharing is limited, there are no open anyone links, and groups and teams have owners.

External sharing restricted

● **Partly**

SharePoint and OneDrive sharing doesn't allow anyone links.

GAPS

- Anyone, including anonymous links.
 - SharePoint and OneDrive: Anyone links are allowed

Fix: Change SharePoint external sharing to "New and existing guests" so every external person signs in. If the client relies on Anyone links, set them to expire and to view-only.

Text to paste: Anyone, including anonymous links.

What Microsoft 365 can't show: Judged from SharePoint tenant settings.

No anyone links in use

● **Partly**

No files or folders are shared with anyone who has the link.

GAPS

- 2 files and folders shared with anyone.
 - holiday.jpg (OneDrive of anna.kowalski@fabrikam.example): Anyone can view
 - Open day flyer.pdf (Marketing / Documents): Anyone can view, link never expires

Fix: Remove anyone links that are no longer needed, and set the rest to view-only with an expiry date. The Shared files report lists each one.

Text to paste: 2 files and folders shared with anyone.

What Microsoft 365 can't show: Judged from SharePoint and OneDrive sharing links.

Guest users reviewed

● **Pass**

Guest accounts are reviewed, and invitations nobody accepted are removed.

WHAT WE FOUND

- No stale guest invitations.

Text to paste: Guest and external user accounts are not reviewed regularly. 1 guest account: 1 guest inactive for 90+ days or never signed in (g#EXT#@fabrikam.example).

What Microsoft 365 can't show: Judged from Entra ID guests and their invitation state.

Every group and team has an owner

● Partly

Microsoft 365 groups and teams have owners who answer for their membership and content.

WHAT WE FOUND

- Unused teams and groups expire after 365 days.

GAPS

- 4 teams and groups without an owner.
 - Project Phoenix: Team, only owner is disabled (Ben Okafor)
 - Marketing: Microsoft 365 group, only owner is disabled (Ben Okafor)
 - Marketing: Microsoft 365 group, no owner
 - Provisioned: Microsoft 365 group, owned only by an app (Provisioning app)

Fix: Make an active person, ideally two, an owner of each listed team or group (Teams admin center or Microsoft 365 admin center > Teams & groups). Owners approve members and guests and renew the group; without one, nobody looks after its files and conversations. The ownerless group policy (Microsoft 365 admin center > Settings > Org settings > Microsoft 365 Groups) asks members to take over when the last owner leaves.

Text to paste: Unused teams and groups expire after 365 days. 4 teams and groups without an owner.

What Microsoft 365 can't show: Judged from Entra ID groups.

Intune and devices

● Fail

Devices are enrolled, compliant, encrypted and on supported versions.

Devices enrolled and compliant

● Partly

Company computers are managed by Intune, check in, and meet the compliance policies.

GAPS

- 1 of 55 joined computers not in Intune.
 - DESK-RECEPTION: Hybrid joined, not managed by Intune
- 9 of 55 managed devices not compliant.
 - DESK-LEWIS12 (william.lewis@fabrikam.example): Not compliant
 - DESK-MOORE18 (ava.moore@fabrikam.example): Not compliant
 - DESK-ROBINSON51 (owen.robinson@fabrikam.example): Not compliant
 - LAPTOP-DAVIES38 (ruby.davies@fabrikam.example): Not compliant
 - LAPTOP-LEE25 (arthur.lee@fabrikam.example): Not compliant
 - and 4 more
- 5 devices haven't checked in for 30+ days.
 - DESK-LEWIS12 (william.lewis@fabrikam.example): Last check-in 38 days ago
 - DESK-ROBINSON51 (owen.robinson@fabrikam.example): Last check-in 38 days ago
 - LAPTOP-DAVIES38 (ruby.davies@fabrikam.example): Last check-in 38 days ago
 - LAPTOP-LEE25 (arthur.lee@fabrikam.example): Last check-in 38 days ago
 - LAPTOP-OKAFOR (ben.okafor@fabrikam.example): Last check-in 45 days ago

Fix: Enrol Entra-joined and hybrid-joined computers in Intune (automatic enrolment under Devices > Enrollment > Windows) so compliance, encryption and updates can be enforced on them.

Text to paste: 1 of 55 joined computers not in Intune. 9 of 55 managed devices not compliant. 5 devices haven't checked in for 30+ days.

What Microsoft 365 can't show: Judged from Intune and Entra ID.

Disks encrypted

● Fail

Company computers are encrypted.

GAPS

- 6 of 54 computers not encrypted.
 - DESK-MOORE18 (ava.moore@fabrikam.example): Windows disk isn't encrypted
 - DESK-ROBINSON51 (owen.robinson@fabrikam.example): Windows disk isn't encrypted
 - LAPTOP-OKAFOR (ben.okafor@fabrikam.example): Windows disk isn't encrypted
 - LAPTOP-ROBINSON07 (thomas.robinson@fabrikam.example): Windows disk isn't encrypted
 - LAPTOP-WARD29 (jack.ward@fabrikam.example): Windows disk isn't encrypted
 - and 1 more

Fix: Turn on BitLocker (Windows) and FileVault (macOS) with an Intune disk encryption policy, with recovery keys escrowed to Entra ID, so a lost or stolen laptop doesn't expose the client's data.

Text to paste: 6 of 54 computers not encrypted.

What Microsoft 365 can't show: Judged from Intune.

Supported operating systems

● Fail

Windows computers run a version that still gets security updates.

GAPS

- 7 of 54 Windows computers past end of support.
 - LAPTOP-HARRIS31 (noah.harris@fabrikam.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-JACKSON49 (chloe.jackson@fabrikam.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-OKAFOR (ben.okafor@fabrikam.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-SMITH13 (owen.smith@fabrikam.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-WALKER04 (rhys.walker@fabrikam.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - and 31 more

Fix: Upgrade computers on Windows 10 or an old Windows 11 release to the current Windows 11 release (Intune: Windows feature updates policy). Replace hardware that can't run Windows 11, or buy Extended Security Updates as a stopgap.

Text to paste: 7 of 54 Windows computers past end of support.

What Microsoft 365 can't show: Judged from the Windows versions Intune reports.

About this evidence

This is a subset of the benchmark: the recommendations Office Sentry can judge from read-only data. A Pass is evidence for that recommendation; the rest of the benchmark still needs checking in the admin centres.

Requirements: CIS Microsoft 365 Foundations Benchmark, recommendations matched by title. Recommendations paraphrased from the CIS Microsoft 365 Foundations Benchmark. CIS rennumbers them between versions, so match each one by its title in the version you're auditing against. Defender, Purview and Teams meeting settings Office Sentry doesn't read are left out rather than guessed.

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Pass and Fail are judged from Microsoft 365 settings and accounts read with read-only access; nothing was changed. The oldest data used was collected 12 Oct 2026, 06:36 UTC. Accepted risks are exceptions the organisation has reviewed and documented. Complete the [parts in brackets] before using a text.