Employer Set Project Core Skills Study Guide

A generic revision and practical preparation guide for Digital Support and Security ESP-style tasks

Covers project planning, support diagnostics, needs analysis, solution development and reflective evaluation.

Task	Main purpose
Task 1	Plan the project, costs, resources, risks and rationale
Task 2	Diagnose issues, support users, test fixes and document evidence
Task 3	Analyse needs and propose suitable hardware, software and security
Task 4a	Develop a secure, working and scalable technical solution
Task 4b	Evaluate the solution with evidence, limitations and improvements

Generic version - adapt examples to the scenario, roles, locations and files provided in the live assessment.

1. How to use this guide

This document turns ESP-style tasks into a repeatable study and exam approach. It is written generically so it can be applied to different businesses, locations and Packet Tracer scenarios.

Core idea	The ESP is not just a Packet Tracer test. It assesses whether you can read a business scenario, identify technical needs, plan sensibly, troubleshoot methodically, build a working solution and explain your decisions clearly.

When revising, do not only memorise commands. Practise reading a scenario and asking: who needs access, who should be restricted, what data matters, what services are required, and how will I prove the solution works?

Use this section when...	What to focus on
You are preparing for Task 1	Planning, Gantt charts, costs, staff allocation, risk and rationale.
You are preparing for Task 2	Helpdesk questions, troubleshooting flow, test logs and fixing defects.
You are preparing for Task 3	Needs analysis, hardware, software, security risks and mitigations.
You are preparing for Task 4a	Packet Tracer build order, VLANs, routing, wireless, servers, access control and testing.
You are preparing for Task 4b	Evaluation writing, specific evidence, limitations and improvements.

2. The ESP task map

Task	Typical output	What the marker is really looking for
Task 1 - Planning a project	Spreadsheet plan, Gantt chart, costs and rationale PDF	A logical plan with dependencies, realistic timings, sensible staff allocation, accurate cost judgement and justified decisions.
Task 2 - Diagnosing issues	Support ticket responses, test/fix log and corrected simulation	A clear troubleshooting process that a third party could follow, plus evidence that fixes were tested.
Task 3 - Planning a solution	Needs analysis document	A business-aware proposal covering devices, network equipment, media, software, risks, mitigations and justified choices.
Task 4a - Developing a solution	Packet Tracer network/simulation evidence	A working, secure, organised and scalable technical solution that meets user and business requirements.
Task 4b - Reflective evaluation	Evaluation document	A balanced judgement using examples from your own solution, including limitations and improvements.

High-mark pattern	Requirement -> design decision -> evidence -> justification -> limitation -> improvement. Use this pattern across written tasks, especially Task 1 rationale and Task 4b evaluation.

3. Universal exam mindset

Before starting any task, extract the scenario requirements. Most marks are easier to access if you understand the business context first.

Question to ask	Why it matters
What does the organisation do?	The business type affects software, hardware, storage, performance and security needs.
Which departments or roles exist?	Different roles usually need different permissions, VLANs, shared folders or remote access.
Which data is sensitive?	Finance, source code, client records, staff records and backups need stronger protection.
Where are users located?	Multiple offices, remote staff and separate buildings imply routing, wireless coverage, VPN or WAN links.
What services are needed?	Email, shared data, DNS, DHCP, printing, web, cloud backup and remote access may be required.
Who needs to be blocked?	A secure solution includes both allowed access and denied access.
How will I test success?	Every major requirement should have a practical test and a clear expected result.

```
Quick scenario extraction checklist
[ ] Business type
[ ] Locations/offices/buildings
[ ] Departments/staff roles
[ ] Sensitive data
[ ] Shared resources
[ ] Remote/hybrid users
[ ] Wireless users and visitors
[ ] Servers and services
[ ] Backup/recovery needs
[ ] Security restrictions
[ ] Growth/scalability needs
```

4. Task 1 - Planning a project

Task 1 usually checks whether you can plan the implementation of a digital support or infrastructure project. You may be given a spreadsheet, budget, cost information, staff roles and project aims.

4.1 What to produce

Output	What it should show
Gantt chart	Task order, durations, start/end dates, dependencies and parallel tasks.
Resource/cost plan	Equipment, software, staff time, fixed costs, ongoing costs and affordability.
Rationale	Why you made the planning decisions, including dependencies, staff allocation, risks, benefits, timings and cost impact.

4.2 Core Task 1 skills

Skill	What to practise
Gantt chart planning	Break the project into clear stages such as planning, procurement, installation, configuration, testing, training and handover.
Dependencies	Explain what must happen first, such as cabling before device configuration or server installation before user testing.
Staff allocation	Assign tasks based on skill, availability, cost and risk. Do not assign every task to the same person without reason.
Budget control	Compare planned spending with the project budget and ongoing maintenance budget.
Risk and benefit analysis	Explain trade-offs, such as higher cost for better resilience or faster delivery with increased staffing cost.
Rationale writing	Use cause-and-effect language: because, therefore, this reduces, this allows, this prevents.

4.3 Strong rationale sentence patterns

```
I scheduled [task] before [task] because [dependency].
I allocated [staff/role] to [task] because [skill, cost or availability reason].
This reduces the risk of [risk] because [technical/business reason].
The impact on timing/cost is [impact], which is acceptable because [justification].
```

Example: I scheduled network installation before server configuration because the server needs a working network connection before shared storage and permissions can be tested. I allocated the senior technician to server and security configuration because mistakes in those areas could expose sensitive data or delay user testing.

4.4 Common Task 1 mistakes

Mistake	Better approach
Listing tasks with no dependencies	Show which tasks rely on others and which can run in parallel.
Choosing the cheapest option only	Consider performance, security, future growth and business impact.
Ignoring ongoing costs	Include maintenance, support, licensing, training and cloud/backup costs where relevant.
No justification for staff allocation	Explain why a technician, specialist or manager is suited to a task.
Vague rationale	Link every decision to the business aims and technical requirements.

5. Task 2 - Diagnosing issues and providing support

Task 2 normally has two parts. First, you explain how you would support users based on tickets. Second, you test and fix defects in a simulation or network file.

5.1 Activity A - Support ticket responses

For each user issue, write follow-up questions, possible causes and possible fixes. Your answer should be detailed enough that another technician could continue the support process.

Ticket type	Good follow-up questions	Likely causes to consider
Cannot print	Is anyone else affected? Is it one printer or all printers? Does the printer show online? Has it worked before?	Printer IP, network path, queue, permissions, wrong default printer, device offline.
Cannot access email	Is there an error message? Can other services be reached? Does it happen on another device?	Email service down, DNS issue, account/password issue, gateway/network problem.
Cannot save to shared drive	Is the user allowed to write there? Can they read files? Are other users affected?	Folder permission, server access, full disk, network connectivity, wrong user group.
Cannot connect to Wi-Fi	Can other users connect? Is the SSID visible? Is the password correct? Is it staff or guest Wi-Fi?	Wrong SSID/passkey, AP issue, DHCP problem, VLAN/trunk issue, wireless security settings.
No internet for all staff	Can users reach local servers? Can the router reach the ISP? Did it start after a change?	Default route, DNS, router/WAN link, ISP gateway, firewall/ACL blocking traffic.

5.2 Activity B - Troubleshooting flow

Use a layered approach	Start with simple physical and IP checks before jumping to advanced fixes. A working technician isolates the fault logically instead of randomly changing settings.

1. Check physical connectivity: cables, link lights, device power, interface status.
2. Check IP settings: IP address, subnet mask, default gateway and DNS server.
3. Ping the local gateway to confirm the device can leave its own network.
4. Ping a local server or printer to test the local LAN/VLAN.
5. Ping a device on another subnet to test routing.
6. Check server services such as DHCP, DNS, FTP, email, web or file sharing.
7. Check user accounts, group membership and read/write permissions.
8. Check ACLs, firewall rules, VLAN assignment and trunk settings.
9. Apply one fix at a time, retest, then document the result.

5.3 Test log writing template

Column	What to write
Test/issue description	The specific problem being tested, such as Finance PC cannot access finance server.
Test action	The exact action, such as ping 192.168.30.10 or log in as finance user and save test file.
Expected outcome	What should happen if the network is correct.
Actual outcome	What actually happened before or after the fix.
Comments/intended action	What you changed, why, and whether retesting passed.

```
Example test log entry
Issue: Guest laptop can access internal file server.
Test action: From guest Wi-Fi laptop, ping internal file server and attempt FTP/file access.
Expected outcome: Guest device should not reach internal server.
Actual outcome: Guest device can ping server.
Action: Applied ACL to block guest subnet from internal server subnet, then retested.
Retest outcome: Guest device cannot access server but can still reach internet.
```

5.4 Packet Tracer commands and checks to know

Check	Useful commands or places to look
Interface status	show ip interface brief; check green link lights and port status.
VLANs	show vlan brief; check access ports are in the correct VLAN.
Trunks	show interfaces trunk; check switch links or router-on-a-stick links.
Routes	show ip route; check static/default routes and directly connected networks.
DHCP	Check DHCP pools, excluded addresses and whether clients receive addresses.
ACLs	show access-lists; check direction and interface placement.
Device IP settings	Desktop > IP Configuration, or ipconfig on PCs.
Services	Server > Services: DHCP, DNS, FTP, email, web, etc.

6. Task 3 - Planning a solution / needs analysis

Task 3 is about turning a scenario into a technical proposal. You are not just listing devices. You are showing that each device, service, software choice and security control meets a real business need.

6.1 Needs analysis structure

```
For each recommendation, use:
Need -> hardware/software -> reason -> risk -> mitigation

Example:
The finance team needs secure access to payroll and billing data. A finance VLAN and restricted file server permissions
```

6.2 Hardware/device ideas

Category	Examples	Why they may be needed
End devices	Desktop PCs, laptops, tablets, printers, IP phones	Allow users to complete work, communicate, print and access resources.
Intermediate devices	Switches, routers, wireless access points, firewall	Connect devices, route between networks, provide wireless and control traffic.
Servers	File, DNS, DHCP, web, email, backup, authentication	Provide central services, shared data, addressing, name resolution and recovery.
Network media	Ethernet, fibre, patch panels, wall ports, wireless	Provide reliable connectivity and enough bandwidth for the work being done.
Security hardware	Firewall, lockable cabinet, UPS, CCTV/access control if relevant	Protect availability, confidentiality and physical access to infrastructure.

6.3 Software ideas

Software type	Examples	Justification angle
Operating systems	Windows desktop/server, Linux server	Compatibility, user familiarity, central management and service hosting.
Productivity	Office suite, email client, collaboration tools	Document creation, communication and daily business operations.
Specialist tools	Design software, development tools, accounting software, CRM	Chosen based on the business type and department needs.
Security	Antivirus/EDR, firewall management, MFA, password manager	Protects against malware, unauthorised access and poor account security.
Backup/recovery	Backup software, cloud backup client, restore tools	Supports business continuity and recovery after data loss.
Monitoring/support	Asset management, ticketing, network monitoring	Helps support staff maintain the environment and diagnose issues.

6.4 Scenario clues and what they imply

Scenario clue	Likely technical implication
Different departments or staff roles	Use role-based permissions, possibly VLANs/subnets and group access controls.
Finance, HR or management data	Restrict access, use strong authentication, backups and clear audit/permissions.
Source code or design files	Protect intellectual property using restricted folders, backups and limited access.
Visitors need Wi-Fi	Separate guest Wi-Fi from internal staff networks.
Staff work remotely or visit clients	Provide secure remote access, laptops and least-privilege access.
Separate building or office	Plan routing, cabling, wireless coverage, inter-site links and redundancy.
Business growth	Allow spare switch ports, scalable IP ranges and upgradeable infrastructure.
Shared data across offices	Use file servers, VPN/WAN links, DNS and permissions.

6.5 Security risks and mitigations

Risk	Mitigation
Unauthorised access to sensitive files	Role-based permissions, separate VLANs, ACLs, strong passwords and MFA.
Guest users reaching internal systems	Guest SSID/VLAN with ACL blocking internal subnets; internet-only access.
Data loss from deletion, corruption or ransomware	Regular backups, tested restores, limited write access and security software.
Weak wireless security	WPA2/WPA3, strong passphrases, separate staff/guest networks, password rotation.
Physical access to servers/network kit	Locked rooms/cabinets, restricted access, visitor controls and UPS.
Single point of failure	Backups, spare capacity, documented recovery plan and redundant links where practical.
Poor documentation	Naming conventions, IP plan, test evidence and maintenance notes.

7. Task 4a - Developing a solution

Task 4a is usually the most practical part. You may need to build, extend or secure a network simulation. The strongest solutions are not only working; they are organised, secure, scalable and easy for another technician to understand.

7.1 Build order

1. Read the full brief and extract roles, locations, data, services and restrictions.
2. Sketch a quick design: subnets/VLANs, routers, switches, servers, wireless and WAN links.
3. Name devices clearly before configuring them.
4. Configure physical topology and cabling.
5. Configure VLANs and access ports if segmentation is needed.
6. Configure trunks and router-on-a-stick or layer 3 routing if required.
7. Configure IP addresses, DHCP pools and static addresses for servers/printers/routers.
8. Configure routing between networks/offices and default routes toward the internet/ISP.
9. Configure servers and services: DHCP, DNS, FTP/file, web, email or backup where needed.
10. Configure wireless: staff SSID and guest SSID, with security and separation.
11. Configure ACLs/security rules to allow required access and block unnecessary access.
12. Test every requirement, fix defects and keep evidence for Task 4b.

7.2 Generic VLAN/IP plan example

Use simple, consistent addressing. The exact numbers do not matter as much as clarity, correctness and scenario fit.

Purpose	VLAN	Example subnet	Gateway
Management	10	192.168.10.0/24	192.168.10.1
Admin/Support	20	192.168.20.0/24	192.168.20.1
Finance	30	192.168.30.0/24	192.168.30.1
Designers/Programmers	40	192.168.40.0/24	192.168.40.1
Guest Wi-Fi	50	192.168.50.0/24	192.168.50.1
Servers	60	192.168.60.0/24	192.168.60.1

7.3 Access control patterns

Rule	Reason
Guest VLAN can access internet only, not internal servers	Visitors should not see business systems or data.
Finance VLAN can access finance server; other departments cannot	Protects payroll, billing and budget data.
Management can access key department data	Supports oversight and decision-making.
Programmers/designers can access source/design server	Allows job tasks while protecting intellectual property.
Admin/support access is limited to their required systems	Applies least privilege.
Remote users can access only the services they need	Reduces risk if remote credentials/device are compromised.

7.4 Naming conventions

Consistent names make your network easier to mark, troubleshoot and evaluate.

```
Example names
R-HQ-01
R-BRANCH-01
SW-FINANCE-01
SW-SERVER-01
AP-STAFF-01
AP-GUEST-01
SRV-DHCP-DNS-01
SRV-FILE-01
SRV-BACKUP-01
VLAN10-MGMT
VLAN20-ADMIN
VLAN30-FINANCE
VLAN40-DESIGN
VLAN50-GUEST
VLAN60-SERVERS
```

7.5 Testing matrix

Requirement	Test	Pass condition
Users receive IP addresses	Check IP configuration on PCs/laptops	Correct IP, subnet, gateway and DNS are assigned.
Inter-VLAN routing works	Ping between allowed VLANs	Allowed VLANs can communicate.
Restricted VLANs are blocked	Attempt ping/file access from blocked VLAN	Traffic fails as intended.
Staff Wi-Fi works	Connect staff laptop to staff SSID	Laptop gets IP and reaches required resources.
Guest Wi-Fi is isolated	Connect guest device and test internal access	Guest reaches internet only, not internal servers.
Shared files work	Log in as correct user and read/write test file	Correct permissions apply.
Backup path works	Ping/access backup server or simulated cloud server	Backup destination is reachable by authorised systems.
Remote/site access works	Test from remote/branch device to allowed internal service	Allowed connection works; blocked access fails.

7.6 Common Task 4a mistakes

Mistake	Why it loses marks
Everything is on one flat network	It may work, but it ignores security, departments and visitor isolation.
Guest Wi-Fi can access internal servers	Fails basic confidentiality and network segmentation.
No consistent IP plan	Hard to maintain, troubleshoot or justify.
Only testing ping	Ping does not prove file permissions, DNS, Wi-Fi separation or service access.
ACL placed on wrong interface/direction	The rule may not protect the network, or it may block legitimate traffic.
No spare capacity	Weak scalability if the scenario mentions business growth.

8. Task 4b - Reflective evaluation

Task 4b is where you prove you understand your own solution. Do not just say that it works. Explain how well it meets the requirements, using specific evidence from your design and tests.

8.1 Evaluation structure

```
Use this pattern:
Requirement -> what I configured -> evidence/test -> judgement -> limitation -> improvement

Sentence starter:
The solution [meets/partly meets/does not fully meet] the requirement for [requirement] because I configured [specific
```

8.2 Example evaluation paragraphs

Example 1 - visitor access: The solution meets the requirement for visitor wireless access because I created a separate guest wireless network. The guest device can connect and reach the internet, but cannot access the internal file server. This protects internal data while still giving visitors basic connectivity. The solution could be improved by adding a documented process to regularly change the guest Wi-Fi password.

Example 2 - department security: The solution partly meets the requirement for protecting sensitive department data because finance users can access the finance server while general users are blocked. However, the solution relies mainly on network-level controls. It could be improved by also applying stronger file permissions, user groups and audit logs on the server.

Example 3 - scalability: The solution supports growth because each department has its own subnet and the switches have spare ports for extra users. However, there is limited redundancy. A future improvement would be to add a secondary link or backup route so one link failure does not disconnect the office.

8.3 Improvements you can mention

Improvement	When it is relevant
Additional backup link or redundancy	When a single router, switch or WAN link is a single point of failure.
Stronger ACLs or firewall rules	When departments/guests need tighter separation.
MFA for remote access	When users connect remotely to internal resources.
Improved backup schedule and restore testing	When data loss or recovery is a key risk.
Network monitoring	When ongoing support and maintenance are important.
Better documentation	When another technician must maintain the system.
More scalable switches/IP plan	When the business is growing or adding departments.

9. Hidden and inferred skills across all tasks

ESP scenarios often imply requirements instead of stating them directly. This is where higher-quality answers stand out.

Implied clue	What a strong student infers
Departments with different job roles	Use role-based access, permissions and possibly VLANs.
Management, finance or HR	Restrict sensitive records and allow management oversight where appropriate.
Programmers/designers/source code	Protect intellectual property with restricted access, backups and controlled sharing.
Reception or public areas	Consider visitor access, physical security and locked devices.
Cleaners, visitors or contractors	Use physical security, screen locking and guest networks.
Staff use either office space	Use consistent authentication, shared resources and routing between locations.
Staff travel or work from home	Use secure remote access and least privilege.
External/cloud backup	Plan backup route, authorised access and recovery testing.
Increased network traffic	Use better switches, structured cabling, scalable IP plan and bandwidth awareness.
A third party must understand the work	Use clear names, documentation, test evidence and logical organisation.

10. Core technical skills checklist

```
Networking fundamentals
[ ] IP addresses, subnet masks and default gateways
[ ] Static IPs for routers, servers and printers
[ ] DHCP pools and excluded addresses
[ ] DNS basics and name resolution
[ ] Static routes and default routes
[ ] Inter-VLAN routing

Segmentation and security
[ ] VLAN creation and port assignment
[ ] Trunk ports
[ ] Router-on-a-stick/subinterfaces
[ ] ACL allow/block rules
[ ] Staff and guest wireless separation
[ ] Least privilege and role-based access

Services and support
[ ] File/FTP services and user permissions
[ ] Email/web service basics
[ ] Printer configuration and testing
[ ] Backup server/cloud backup concept
[ ] Remote access/VPN concepts
[ ] Test logs and evidence writing
```

11. Practical revision labs

The best preparation is to build small networks repeatedly, break them, and fix them. Aim for speed and confidence, not one perfect giant network.

Lab	Build	Tests to complete
Lab 1 - Department office	Management, Admin, Finance, Guest Wi-Fi, file server and printer	Finance can access finance data; guests cannot access internal server; all allowed users can print.
Lab 2 - Design/software company	Programmers/designers, source-code server, shared media server, backup server	Programmers can access source code; other users are restricted; backup server is reachable.
Lab 3 - Two offices	Two routed LANs with servers in each office	Office A reaches Office B services; routes and gateways are correct.

Lab	Build	Tests to complete
Lab 4 - Troubleshooting	Take a working network and deliberately break one thing at a time	Identify and fix wrong gateway, missing route, wrong VLAN, ACL issue, DHCP issue and service-off issue.

12. Two-week revision plan

Day(s)	Focus	Outcome
1-2	Scenario reading and Task 1 planning	Practise extracting requirements and creating a short Gantt/cost rationale.
3-4	IP addressing, DHCP and static routing	Build small routed networks until gateway/route issues feel routine.
5-6	VLANs, trunks and inter-VLAN routing	Build a multi-department LAN with a clean IP plan.
7	ACLs and role-based access	Allow required traffic and block restricted access.
8	Wireless and guest isolation	Create staff and guest wireless networks with correct separation.
9	Servers and services	Configure DHCP, DNS, file/FTP, email/web or backup services as needed.
10	Task 2 troubleshooting	Use a test log to fix deliberately broken networks.
11	Task 3 needs analysis	Write hardware/software/security recommendations from a scenario.
12	Task 4a full mini build	Build a complete small office solution from a brief.
13	Task 4b evaluation	Evaluate the mini build using evidence and improvements.
14	Timed practice	Attempt a mixed mock under time pressure and review weaknesses.

13. Final exam checklist

Before submission Check that the files are named correctly, saved in the correct format, and that every required output has been completed. A working solution can still lose marks if the evidence is unclear or missing.

```
Task 1
[ ] Gantt chart complete
[ ] Costs calculated
[ ] Budget/affordability considered
[ ] Staff allocated sensibly
[ ] Rationale explains dependencies, risks, benefits, timings and costs

Task 2
[ ] Support questions are specific
[ ] Possible causes are realistic
[ ] Possible solutions are practical
[ ] Test log shows expected vs actual results
[ ] Fixes were retested

Task 3
[ ] End devices included
[ ] Intermediate devices included
[ ] Network media included
[ ] Software included
[ ] Security risks included
[ ] Mitigations included
[ ] Suggestions are justified

Task 4a
[ ] Devices named clearly
[ ] IP plan is consistent
[ ] VLANs/subnets configured where needed
[ ] Routing works
[ ] Wireless works and guests are separated
```

```
[ ] Servers/services work
[ ] Permissions/security rules work
[ ] Requirements tested

Task 4b
[ ] Evaluation refers to requirements
[ ] Specific examples from your solution are included
[ ] Limitations are honest
[ ] Improvements are realistic
[ ] Judgements are explained
```

14. One-page memory summary

Remember	Meaning
Read the business first	Do not start configuring until you know who needs what.
Access is both allow and block	A secure design says who can access data and who cannot.
VLANs need a reason	Use VLANs for departments, guests, servers or sensitive data - not just because they sound advanced.
Ping is not enough	Also test DNS, file access, Wi-Fi, permissions, printing, backup and blocked access.
Document like another technician will read it	Clear names, clear test logs and clear justifications gain marks.
Evaluation needs evidence	Refer to what you actually configured and tested.

Best exam mindset Build a solution that is functional, secure, scalable, maintainable and clearly justified. That combination is stronger than a messy network with a few advanced features.

End of guide