# Change Rationale

The previous flat network allowed all internal systems to communicate freely, meaning that one compromised workstation could quickly spread malware or access sensitive data.
The redesigned topology separates the environment into the DMZ, Trusted, and Front Desk VLANs, enforcing a default-deny posture between them. Only the Web Server may reach the Database on a single required port (3306), while Front Desk systems are blocked entirely from critical assets.
This enforces least privilege and limits the blast radius of any attack.
If the Internet→Web rule were removed, customers couldn't reach the site; if the Web→DB restriction were loosened, attackers could exfiltrate data; and if Front Desk→Trusted were opened, phishing-infected PCs could reach the Database.
The new configuration therefore balances business functionality with security, aligning with NIST CSF and CIS Controls and achieving true Defense in Depth.