1. استفاده از خطوط شهری پیش پرداخت (بالا)
2. استفاده از رمز های با طول بیشتر از 12 کاراکتر و تا به حال استفاده نشده (بالا) (الزامی)
3. مشاهده و بررسی لاگ ها تلفنی (بالا)(الزامی)
4. بستن درسترسی به شماره های بین الملل بر روی خط شهری از سمت سرویس دهنده(بالا)(الزامی-توصیه)
5. به روز رسانی مداوم برنامه ها (الزامی)
6. تغییر پورت SIP بر روی روتر ورودی سازمان (الزامی)
7. بستن امکان Post Scaning بر روی روتر ورودی (الزامی)
8. تغییر پورت SSH
9. تغییر پورتSSL (الزامی)
10. قراردادن رمز بر روی آپاچی (الزامی)
11. تغییر پورت AMI روی استریسک
12. بستن دسترسی به ایزابل از خارج ایران بر روی ایزابل توسط Iptables Addons
13. استفاده و تنظیم درست Fail2Ban برای جلوگیری از BruteForce (الزامی)
14. استفاده از TLS برای امن سازی پروتکل SIP
15. استفاده از SRTP برای امن سازی پروتکل RTP وجلوگیری از شنود
16. نصب و تنظیمم OpenVPN بر روی ایزابل برای دسترسی کاربران
17. اعمال نکات امنیتی بر روی محیط وب ایزابل و تنظیمات تلفنی نظیر ترانک، داخلی و ...