Controls & Compliance Assessment

Scenario

(This is based on a fictional company)

NovaTech Solutions is a mid-sized South African software development and IT consulting firm that provides custom applications for both local and international clients. The business operates out of a single headquarters in Cape Town, which contains executive offices, a development floor, and an on-site server room. NovaTech Solutions has grown rapidly in the last 18 months due to increased demand for remote collaboration tools, which has led to a substantial expansion of its cloud-based services and client database.

With this growth, the IT Director has expressed concern over the company's ability to maintain a secure environment for its critical systems, sensitive customer information, and intellectual property. She believes a **comprehensive internal IT audit** is needed to identify weaknesses, ensure compliance with relevant regulations (including the EU's GDPR), and create a roadmap for improving the organisation's security posture.

The IT Director has decided to align the audit with the **NIST Cybersecurity Framework (NIST CSF)**, beginning with asset identification, classification, and risk assessment. The objective is to determine what controls are currently in place, identify missing or insufficient ones, and ensure compliance with best practices and regulatory standards.

Scope, Goals, and Risk Assessment Report

Scope

The scope covers the **entire security program** at NovaTech Solutions, including both physical and digital assets, internal procedures, employee access policies, and data protection measures.

Goals

- Assess current IT and security assets.
- Complete a **Controls and Compliance Checklist** to determine where gaps exist.
- Recommend practical measures to improve NovaTech Solutions' security posture and reduce exposure to risk.

Current Assets

Assets under the IT department’s management include:

- **On-premises infrastructure**: Servers, network switches, firewalls, and storage systems.
- **Employee devices**: Desktops, laptops, smartphones, tablets, headsets, and peripheral equipment.
- **Cloud-based platforms**: Development environments, project management tools, source code repositories, and client portals.
- **Critical systems**: Accounting software, CRM systems, email servers, database systems, and security monitoring tools.
- **Physical security systems**: Key card entry system, CCTV cameras, biometric scanners for server room access.
- **Internet connectivity and internal network infrastructure**.
- **Data storage solutions**: Both on-premises and in the cloud.
- **Legacy applications** used by long-term clients that require ongoing patching and manual oversight.

Risk Assessment

Risk Description

NovaTech Solutions currently lacks **standardised asset tracking** and **uniform enforcement of access controls**. While some security measures are in place, gaps exist in encryption, backup management, and intrusion detection. Additionally, the company is not fully compliant with all applicable GDPR requirements for its European client base.

Control Best Practices

The first step in the NIST CSF - **Identify** - is critical for NovaTech Solutions. The company must establish a clear, up-to-date asset inventory, classify data sensitivity, and understand the impact of losing specific assets or systems.

Risk Score

On a scale from 1 to 10, the risk score is **7.5**. While NovaTech has invested in some core security technologies, several critical controls are absent or inconsistently applied.

Additional Comments

- **Impact rating**: Medium to high - Certain system outages could halt core business operations.
- **Regulatory exposure**: High - Non-compliance with GDPR could lead to significant fines.
- **Operational gaps**: Incomplete disaster recovery and incident response plans leave the company vulnerable in the event of a cyberattack or infrastructure failure.

Controls Assessment Checklist

Yes / No / ?	**Control**	**Explanation**
No	Least Privilege	Developers and junior staff currently have access to production databases, increasing the risk of data leaks.
No	Disaster Recovery Plan	No documented disaster recovery plan exists. Recovery processes are ad hoc.
Yes	Firewall	A next-gen firewall is configured but not regularly reviewed for outdated rules.
?	Password Policies	Password complexity rules exist but lack multi-factor authentication enforcement.
Yes	Antivirus	Managed antivirus is deployed across endpoints and updated daily.
No	Backups	Backups are irregular and not encrypted. No off-site redundancy is in place.
No	Encryption	Sensitive client data is not consistently encrypted at rest.
No	IDS	No intrusion detection or prevention systems are in place for internal networks.
Yes	Physical Access Controls	Server room access is restricted via biometric authentication.
Yes	CCTV	Cameras are functional and monitored, but footage retention policies are unclear.
Yes	Fire Detection	Smoke detectors are installed and linked to a building-wide alert system.

Compliance Checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes / No / ?	**Best Practice**	**Explanation**
No	Restrict credit card data access	Payment processing is outsourced, but logs show full card data stored temporarily in internal systems.
No	Store card data securely	Card data is not tokenised or encrypted before temporary storage.
No	Encrypt transmissions	Data is transmitted without end-to-end encryption in some workflows.

General Data Protection Regulation (GDPR)

Yes / No / ?	**Best Practice**	**Explanation**
No	Protect EU customer data	EU customer data is not segregated from other datasets, making targeted compliance difficult.
Yes	Maintain privacy policy	Privacy policy is up-to-date and publicly available.

System and Organization Controls (SOC)

Yes / No / ?	**Best Practice**	**Explanation**
No	User access policies	No formalised role-based access controls are in place.
Yes	Data integrity	Automated checks verify data accuracy in key systems.
No	Limit data access to authorised users	Sensitive source code and client documents are accessible to all developers.

Recommendations

Following this audit, NovaTech Solutions should prioritize:

1. **Implementing least privilege access controls**
   Limit data and system access to only those who require it.

2. **Developing a formal disaster recovery and incident response plan**
   Include backup testing and recovery timelines.

3. **Enforcing multi-factor authentication**
   Enforced across all systems handling sensitive data.

4. **Encrypting all sensitive data**
   Encryption both in transit and at rest.

5. **Deploying an Intrusion Detection System (IDS)**
   To monitor and respond to suspicious activity.

6. **Achieving GDPR compliance**
   Achieved by segmenting EU customer data and applying required safeguards.

By addressing these issues, NovaTech Solutions can significantly improve its security posture, reduce regulatory exposure, and ensure continuity of operations in the face of cyber threats or technical failures.