■Q1 A 【ポイント】：Oracle のバックアップを RMAN（リカバリマネージャ）で取得。S3 に格納している。Storage Gateway ボリュームゲートウェイ（https://aws.amazon.com/jp/storagegateway/volume/ ）を使用している。RTO（Recovery Time Objective：目標復旧時間）を Best に（短く）したい。（選択肢の内容から判断して）オンプレミスの災害時には AWS クラウド上でバックアップシステムを運用する。

A：正しい。EC2上で稼働させたOracleではRMANバックアップを利用できる。Storage Gatewayボリュームゲートウェイでは、バックアップデータをEBSスナップショットとして利用できる。そこからEBSボリュームを作成することができる。
B：正しくない。RDSでは、RMANを使用できない（https://blogs.oracle.com/pshuff/amazon-rds ）。また、Glacierを使用すると復元に時間がかかる（通常、アーカイブ状態から復元を行ってファイルにアクセスできるようになるまで3-5時間がかかる）。
C, D：正しくない。EC2 に Storage Gateway をセットアップする時間がかかる。

■Q2 C【ポイント】：RTO（Recovery Time Objective：目標復旧時間）は 3 時間未満、RPO（Recovery Point Objective：目標復旧時点）は 15 分未満としたい。データの corruption（破壊）が 1.5 時間前に発生し、それを解決する必要がある。（選択肢の内容から判断して）データベースのバックアップをどのように取るかを考えている。

A：正しくない。Glacierからの復元には通常3〜5時間がかかる。
B：正しくない。同期レプリケーションでは、データベースを過去の時点に戻すことはできない。
C：正しい。 1 時間ごとに取られたバックアップのいずれかと、トランザクションログを組み合わせて、データベースのPITR（Point in Time Recovery）を実行できる。
D：正しくない。インスタンスストアは揮発性であるためバックアップの配置場所としては適当ではない。

■Q3 B 【ポイント】：DynamoDB に 80 文字の投稿を行うモバイルアプリを JavaScript で開発する。コスト効率が良くスケーラブルなアーキテクチャにしたい。

A、C：正しくない。Web IDP（IDプロバイダ）を使用すれば、TVM（https://aws.amazon.com/jp/articles/authenticating-users-of-aws-mobile-applications-with-a-token-vending-machine/ 参照、STSにアクセスして一時的認証情報を返す）を使用する必要はない。
B：正しい。AWS SDK for JavaScriptを使用して開発。S3（静的ウェブホスティング有効化）から配信。モバイルアプリはWeb IDPと使用して一時的認証情報を取得する（実装としてはCognitoを使用できる）。モバイルアプリから一時的認証情報を使用して、直接DynamoDBへ書き込む。
D：正しくない。モバイルアプリを EC2 インスタンスから配布するのは、S3 を使用する場合よりもコストがかかる。また EC2 インスタンスは DynamoDB に Put する必要はない。

■Q4 D【ポイント】：機密情報を扱うウェブサイトであり、SSL の処理が必要。SSL 秘密鍵の流出リスクをなくしたい。サーバーログも暗号化して保存する。
（選択肢の内容から判断して）ELBを使用する。（が、ELBでHTTPS負荷分散をするとは限らない）

A：正しくない。
B：正しくない。秘密鍵をS3バケットに配置したり、EC2にコピーしたりすると、秘密鍵が流出するリスクがある。
C：正しくない。S3のサーバーサイド暗号化を使用すると、ログは「保管時に」S3バケットに暗号化して保存されるが、「転送時」には暗号化されない（選択肢内では、転送時の暗号化については特に言及されていない）。
D：正しい。EC2 上の Web サーバーでの SSL 処理において、CloudHSM を使用したオフロードができる。

※なお、ログを ephemeral volume（インスタンスストア）に格納すると、インスタンス終了時にクリアされてしまうため、これ自体はベストプラクティスとは言えない。

■Q5 D【ポイント】：ビジネス旅行者向け（おそらく、特定の会社の社員向け、出張時に利用する）の FAT クライアントアプリケーション用のネットワークを設計している（FAT クライアント=PC 上にインストールされる高機能アプリケーション。THIN クライアント＝Web アプリケーション）。ホテルの部屋やインターネットなどのさまざまな場所からアクセスする必要がある。アプリケーションはインターネットに公開しない。デプロイと運用コストを最小化したい。（選択肢の内容から判断して）Direct Connect 接続、ELB、IPsec VPN 接続、SSL VPN 接続のいずれかを使用する。

A、C：正しくない。インスタンスをパブリックサブネットに配置するとインターネットに公開されてしまう。またAはDirect Connectのコストがかかる。Cは、OSレベルでIPsecの設定を各社員PCで個別に設定する必要があり、運用コストがかかる。
B：正しくない。ELB（+SSLリスナー）を使用するということは、ELBはインターネットに公開されてしまう。
D：正しい。クライアント側ではOpenSSL VPNクライアントソフトウェアをセットアップして使用することができる。サーバー側ではOpenSSL VPNサーバーをセットアップしたインスタンスをパブリックサブネットに配置する。アプリケーションはプライベートサブネットに配置する。

■Q6 B【ポイント】：オンプレミスのレガシーアプリケーションを AWS に移行する。条件は「週末に以降できること」。インターネット接続を使用した場合は「最低 48 時間」の転送時間が見込まれている。

A：正しくない。週末からコピーを開始すると、翌週の業務開始までに間に合わない可能性がある。
B：正しい。「aws s3 sync」コマンドを使用して、オンプレミスと S3 で同期を行うことができる。選択肢の中で最も確実な方法である。
C：正しくない。Import/Export Disk(https://aws.amazon.com/jp/snowball/disk/details/ )を使用すると、外付け HDD のようなディスクを使用して、オンプレミスから AWS にデータを転送し、EBS スナップショットまたは S3 にデータを格納することができる（が、現在は Snowball を推奨）。Import/Export Disk の「よくある質問」によれば「データの読み込みは、デバイスがデータセンターに到着した後に開始されます。」とあるが、完了する時刻は不明である。
D：正しくない。週末からコピーを開始すると、翌週の業務開始までに間に合わない可能性がある。