Ministerium für Kultus, Jugend und Sport
Baden-Württemberg

Baden-Württembergischer
Industrie- und Handelskammertag
Baden-Württembergischer
Handwerkstag

Schriftliche Abschlussprüfung

Sommer 2016

der

Berufsschulen und zuständigen Stelle(n)

Ausbildungsberuf	IT-Systemkaufmann/-kauffrau	(26)
Prüfungsfach/-bereich	Ganzheitliche Aufgabe I	
Prüfungszeit	90 Minuten	

Verlangt	Alle Aufgaben
Zu beachten	Sind Anlagen beigefügt, können diese abgetrennt werden.
Erlaubte Hilfsmittel	PC mit entsprechender Softwareausstattung

Punkte

Aufgabe 1 **20**

Das Unternehmen NET-Serve fertigt und vertreibt NAS-Systeme (Network Attached Storage). Dazu bezieht das Unternehmen u. a. auch das Gehäuse von einem Zulieferer, wobei insgesamt 190.400 EUR (brutto) an Anschaffungskosten anfallen. Der Lieferant gewährt Skonto in Höhe von 2 % bei Zahlung innerhalb von 10 Tagen und einem Zahlungsziel von 40 Tagen.

1.1 Berechnen Sie den effektiven Jahreszinssatz, wenn Skonto nicht in Anspruch genommen wird. (mit Rechenweg)

1.2 Berechnen Sie die Kostenersparnis, wenn Sie Skonto in Anspruch nehmen und für den notwendigen Betrag kurzfristig ein Kontokorrentkredit zu 14 % (p. a.) benötigt wird. (mit Rechenweg)

1.3 Zur Anschaffung einer Maschine über 200.000 EUR (brutto), deren betriebsgewöhnliche Nutzungsdauer 8 Jahre beträgt, schlägt ein Mitarbeiter vor, das Kontokorrentkonto zu überziehen anstatt einen Darlehensvertrag abzuschließen.

1.3.1 Beurteilen Sie diesen Vorschlag.

1.3.2 Die Hausbank bietet für die Anschaffung der obigen Maschine folgende Darlehen an:

(A) Abzahlungsdarlehen: Zinssatz 6 % (p. a.) nachschüssig, Laufzeit 8 Jahre
(B) Annuitätendarlehen: Zinssatz 6 % (p. a.) nachschüssig, Laufzeit 8 Jahre

Berechnen Sie mit Hilfe der vorliegenden Excel-Tabelle (Finanzierung_leer.xls) die Tilgungspläne für das Annuitäten- und das Ratendarlehen. Verwenden Sie kopierfähige Formeln in Ihrer Lösung.

Hinweis: Annuität $= K * \frac{(1+p)^n * p}{(1+p)^n - 1}$ p = Zinssatz, n = Laufzeit, K = Kreditsumme

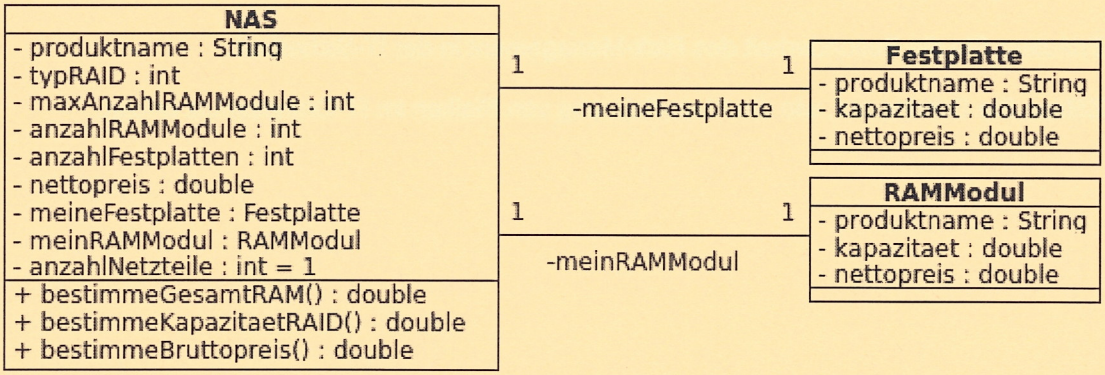
1.4 Erläutern Sie, für welche der Darlehensarten Sie sich entscheiden würden.

Punkte

Aufgabe 2 20

Die Firma Net-Serve stellt NAS-Dateiserver (Network Attached Storage) her. Die Produkte NAS besitzen alle ein Netzteil. Grundsätzlich werden alle NAS mit identischen Festplatten verkauft. Die Anzahl der RAM-Speichermodule ist begrenzt, allerdings sind nicht immer alle Speichersteckplätze belegt. Grundsätzlich gilt auch hier, dass alle Speicherplätze mit identischen Speichermodulen bestückt sind. Die Festplatten des NAS ermöglichen ein RAID der Kategorie 0 oder 1.

Zur Verwaltung der Produkte wurde das im Schaubild dargestellte objektorientierte Modell entworfen. Auf die Angabe der set- und get-Methoden, die sich unmittelbar aus den Attributen ergeben, wurde in diesem Klassendiagramm verzichtet.



2.1 Benennen Sie das statische Attribut dieses Modells. Erläutern Sie, weshalb es sinnvoll ist, dass dieses Attribut statisch ist.

2.2 Erklären Sie den Begriff der Assoziation und gehen Sie auch auf die Begriffe Navigation und Multiplizität am Beispiel der Assoziation zwischen NAS und Festplatte ein.

2.3 Programmieren Sie die Klasse NAS vollständig in der Programmiersprache, die im Unterricht eingeführt wurde. Auf die Programmierung von set- und get-Methoden kann verzichtet werden, diese stehen aber für die folgenden Methoden zur Verfügung.

Die Methode berechneBruttopreis() bestimmt den Bruttopreis eines NAS, der sich aus dem Nettopreis des NAS ergibt, allerdings ohne den darin enthaltenen Speichermodulen und Festplatten. Das Attribut „nettopreis“ stellt den Nettopreis des NAS ohne Festplatten und RAM-Module dar.

Die Methode bestimmeGesamtRAM() bestimmt die Kapazität des RAMs im NAS unter Berücksichtung aller verbauten RAM-Module.

Die Methode bestimmeKapazitaetRAID() bestimmt den verfügbaren Speicherplatz des RAIDs unter Berücksichtigung der Kapazität der einzelnen Festplatten, der Anzahl der Festplatten und des RAID-Typs (0 oder 1).

2.4 Die Firma Net-Serve beschließt auch NAS anzubieten, in denen RAM-Module betrieben werden können, die nicht alle die gleiche Kapazität haben. Erläutern Sie, wie das Softwaremodell angepasst werden muss, damit solche NAS ebenfalls erfasst werden können.

Punkte

Aufgabe 3 **20**

Die Firma NET-Serve bietet neben den RAID Level 0 oder 1 zukünftig auch die Konfigurationen 5 und 10 an.

3.1 Erläutern Sie die vier RAID – Konfigurationen.

3.2 Erläutern Sie die Unterschiede zwischen einem SAN und einer NAS.

3.3 Ein IT-Grundschutz wird immer wichtiger. Beantworten Sie die unten stehenden Fragen mit Hilfe von der Anlage.

3.3.1 Worin liegt die große Herausforderung beim Etablieren des IT-Grundschutzes?

3.3.2 Erläutern Sie die Besonderheit des Risk-Management in der IT-Sicherheit.

3.3.3 Zählen Sie Schritte auf, wie die Klassifizierung von Risiken im IT-Grundschutz erfolgt.

Anlage

The BSI's ISMS: IT-Grundschutz

1.1. Introduction

The descriptions of an information security management system have been kept very generic in this document and in the ISO standards 27000, 27001, and 27002 and only serve as a framework. In practice, therefore, a great deal of freedom exists for the practical implementation of the generic specifications. The great challenge lies in establishing an ISMS in one's own institution that not only helps to achieve the set security objectives but is also as cost-effective and economic as possible.
The question of how an security concept should be developed for the institution is generally the most difficult one to answer. The main procedures for developing an security concept involve assessing the risk and selecting the correct information security safeguards. Choosing the method of risk assessment is particularly important, since the method selection has a decisive effect on the amount of work required to develop an IT security policy. The procedure according to IT-Grundschutz describes a method that is appropriate for the majority of applications. Compared with classical quantitative risk analysis, it is much more cost-effective and has been tried and tested in practice for many years. As an added bonus, the IT-Grundschutz Methodology not only describes how an ISMS functions in principle but, together with the IT Grundschutz Catalogues, also portrays how specific measures might be implemented in practice.

1.2. The security process in accordance with IT-Grundschutz

All the most common methods, best practice examples and management of information security standards barely differ in the explanations that they provide regarding the security process or the duties of the management. The greatest differences lie in the manner in which the policy for information security is specifically developed, i.e. how the risk assessment is formulated and how the information security safeguards are selected. We shall therefore at hits point describe the basic procedure for developing a policy for information security in accordance with IT-Grundschutz.

1.2.1. Risk assessment

Risk assessment in information security
Risk assessment in information security differs in important areas from classical methods of actuarial mathematics or controlling. Precise calculation of the extent of damages and occurrence probabilities is usually not possible in a "classical" or quantitative risk analysis, since appropriate figures are not available. Even if a calculation is possible, interpreting the results remains very difficult.

Classification of risks

The general requirement for classifying risks is accomplished in IT Grundschutz in the following steps:

1. Orientation to damage scenarios

   Various damage scenarios should be examined in order to describe damages and the negative effects of IT security incidents as vividly as possible, for example:
   - Violation of laws, regulations or contracts
   - Impairment of informational self-determination
   - Physical injury
   - Impaired performance of duties
   - Negative internal or external effects
   - Financial consequences

When running through the scenarios, the damages that can arise due to a loss of confidentiality, integrity or availability should be investigated.

2. Classifying damages: definition of protection requirement categories

Performing a precise calculation of potential damages is in most cases not useful or perhaps even impossible, and is also not necessary for selecting appropriate IT security measures. It is therefore advisable to divide damages into a few classes. Attempting to calculate damage "precisely" can even endanger security in many cases, since this gives the false impression that a particular degree of precision has been achieved and those responsible are lulled into a "false sense of security".

Risk assessment

1. Structure analysis: identification of items to be protected

Within the framework of the structure analysis, the relevant items to be protected, such as information, IT-applications, IT systems, networks, rooms and buildings as well as responsible staff members, must be ascertained for the examined information domain (i.e. area of application or business process).
During the structure analysis, the relationships and dependencies between the individual items to be pro tected must also be described. By recording these dependencies in particular it is possible to identify the effects of information security incidents to business activities to be able to provide an appropriate response.

2. **Assessing the protection requirements:** analysing the effects of information security incidents on the examined business processes
The degree of protection required is determined for each of the values ascertained during the structure analysis.

3. Supplementary security analysis

Application of the procedures in accordance with IT-Grundschutz enables a level of information security to be achieved that is sufficient and appropriate for normal protection requirements. If the protection require ments for a particular area (such as an application or IT system) are higher or if no IT-Grundschutz measures exist for an area, a supplementary security analysis should be performed after IT-Grundschutz has been implemented. The BSI has developed its own method for risk analysis for this purpose that is based on the implementation of IT- Grundschutz. It is described in the BSI standard 100-3 [BSI-3]. Howev er, a classical quantitative risk analysis can also be chosen as the method for the areas concerned. If only a small area of information processing is affected, the effort required for an additional risk analysis is usual ly low. If, for example, only a specific IT system is affected for which no IT- Grundschutz module exists, consultation with the manufacturer or independent IT security consultant about this specific issue can generally already provide enough help to assess the risk and select appropriate information security safeguards. The combination of standard security measures with supplementary risk analysis for those areas whose protection requirements exceed the normal protection requirements is considerably more efficient than a complete quantitative risk analysis. Afterwards, the identified measures must then be integrated and consolidated in the remaining information security process.

1.2.2. Development of the security concept

The IT-Grundschutz Catalogues contain catalogues for typical modules, threats and measures. The modules contain descriptions of threats and standard information security safeguards for typical tasks of the information security management and areas of IT application. They consider the organisational, personnel, infrastructural and technical aspects of information security.