Cybersecurity – Supplier's Frequently Asked Questions

Table of Contents

OBM Related Questions: 10

Cybersecurity – Supplier’s Frequently Asked Questions

Cybersecurity Compliance and Risk Assessment (CCRA):

1. **How many questionnaires are there, and which am I required to complete?**
   There are two legacy questionnaires: NIST SP 800-171 (NIST), the Cybersecurity Questionnaire (CSQ), and the new Cybersecurity Compliance and Risk Assessment (CCRA).

   To align with the Aerospace and Defense (A&D) industry, Lockheed Martin is transitioning to the Cybersecurity Compliance and Risk Assessment (CCRA) and will retire the NIST SP 800-171 (NIST) and Cybersecurity Questionnaire (CSQ) that is hosted in Exostar Partner Information Manager (PIM).

   - **Cybersecurity Compliance and Risk Assessment (CCRA):** The CCRA allows suppliers to complete ONE assessment which would be accepted on a reciprocal basis by DoD Prime contractors, or other companies who recognize the CCRA. For LM, the CCRA will be implemented in a web-based format hosted on Exostar’s **Onboarding Module (OBM)**. LM will begin transitioning to the CCRA starting 1st Quarter of 2024.

   - The **NIST SP 800-171 (NIST)** and **Cybersecurity Questionnaire (CSQ)** hosted on Exostar’s Partner Information Manager (PIM) will be phased out as suppliers are migrated to the CCRA on the Onboarding Module (OBM).

2. **What is the Cybersecurity Compliance and Risk Assessment (CCRA) and why do we need to complete this survey?**
   The CCRA was developed by the Defense Industrial Base Sector Coordinating Council (DIB SCC) Supply Chain Task Force (SCCTF) to drive a common set of cybersecurity requirements that both document compliance and measure risk. It’s intended to reduce the burden on our suppliers, currently being assessed against multiple standards and in varied formats (often with overly complex and outdated cyber requirements).

   More information on the DIB SCC SCCTF adoption of the CCRA can be found on the CyberAssist webpage.

3. **When will LM suppliers be transitioned to the CCRA?**
   LM will begin transition the CCRA beginning 1st Quarter 2024.

   - **New Vendors** – Suppliers that are being onboarded and when applicable will be required to complete the CCRA on Exostar’s Onboarding Module (OBM) as part of the registration process.
   - **Existing Vendors with Expired CSQ, NIST, or SPRS Status** – Suppliers who has an expired CSQ, NIST, or SPRS status will be requested to complete the new CCRA instead of the legacy questionnaires. The requests will be sent from LM/Exostar when the migration begins.
   - **Existing Vendors with active CSQ and NIST** - As the NIST/CSQ expires (1 year from the last submission), the suppliers will be prompted to transition to the CCRA on Exostar’s Onboarding Module (OBM).

4. **How can we complete the new CCRA when we haven't been asked to complete it by LM or Exostar?**
   Suppliers that want to take advantage or be an early adopter of the CCRA can manually migrate over to the CCRA by following the below steps.

   1. An Organization Administrator can navigate to https://portal.exostar.com and log into MAG using Multi-Factor Authentication (MFA)
   2. From the ***My Account*** tab, select ***View Organization Details***
   3. In the ***Organization Details*** section select ***View in Trading Partner Management (TPM)*** link
   4. Click Continue, if asked, to access your organization's TPM profile then from the left-hand navigation menu, select ***Self-Certification***
   5. For the ***Applicability of Cyber DFARS and NIST SP 800-171*** section, select option ***2.a***, ***2.b***, or ***2.c***
   6. For the ***Handling Sensitive Information*** section, select **No**.
   7. Click ***Submit Certifications and Representations*** and then click **Save**.
   8. Toggle your responses back to its original state or as applicable.
      a. ***Applicability of Cyber DFARS and NIST SP 800-171*** section, select **1**, OR
      b. ***Handling Sensitive Information*** section, select ***Yes***
   9. Click ***Submit Certifications and Representations*** and then click **Save**.

   Once saved, you should receive an email with instructions on how to complete the CCRA in OBM.

5. **What is Exostar Onboarding Module (OBM) and how can I get access to it?**
   Exostar Onboarding Module (OBM) will replace Partner Information Manager (PIM) and is the application that will host the CCRA. More information on OBM can be found here.

   Once migrated, suppliers can access the OBM application through Exostar's Managed Access Gateway (MAG) or Trading Partner Manager (TPM).

   See ***Supplier Organization User Guide*** provided on the Onboarding Module Training Resources support page.

6. **How does the CCRA calculate the risk rating and how is it assessed?**
   The Cyber Rating derived from the CCRA is based on a subset of 31 thirty-one NIST SP 800-171 Controls that is separated into 3 Categories: (11) Category 1, (10) Category 2, (10) Category 3.

   Green Rating = (All Category 1, 2, and 3 controls are implemented)

   - Negligible to minimal risks are identified based on response provided. The supplier has a strong performing cyber risk management program.

   Yellow Rating = (All Category 1 implemented AND > 1 Category 2 or 3 implemented)

   - Minimal to moderate risk are identified based on the response provided. The supplier has a Cyber risk management program with good protections in place, but additional risk mitigations are likely required to protect Sensitive Information and/or Government/DOD Controlled Unclassified Information (CUI).

Red Rating = (Less than 11 Category 1 implemented)

- Moderate to significant risks are identified based on the response provided. The supplier has minimal or no cyber risk management program and significant cyber protections are lacking.

7. **How can a supplier improve their Cyber Rating?**
   The Cyber Rating derived from the CCRA is based on a subset of 31 thirty-one NIST SP 800-171 Controls that is separated into 3 Categories: (11) Category 1, (10) Category 2, (10) Category 3.

   To be Green, suppliers must attest that all 31 of the Cyber Security Controls on the CCRA is implemented.

8. **I've completed the CCRA but I am not shown as Compliant with DFARS 252.204-7012. What do I need to do to become compliant?**
   The supplier can attest compliance with DFARS 252.204-7012 through the CCRA (questions 2, 2.a, and 2.b) that all 110 NIST cybersecurity controls are implemented OR for controls not fully implemented, the supplier must have a documented Plan of Action and Milestone (POAM) in your System Security Plan (SSP).

   Questions 2, 2.a, and 2.b must all be answered Yes to be shown as compliant with DFARS 252.204-7012 on the CCRA.

   Note: Part of DFARS Clause 252.204-7012 requirement to rapidly report cyber incidents is for suppliers to have or be able to obtain a DoD-approved Medium Assurance Certificate to report cyber incidents to https://dibnet.dod.mil. Question 2.c, though not required for CCRA compliance determination, is required to be compliant with the Clause.

9. **I've completed the CCRA, but I am not shown as Compliant with DFARS 252.204-7019/ -7020. What do I need to do to become compliant?**
   The supplier can attest compliance with DFARS 252.204-7019/ -7020 through the CCRA (questions 3, 3.a, 3.b, and 3.c) that the supplier completed an assessment using the NIST SP 800-171 DoD Assessment Methodology and submitted the score to the DoD-managed Supplier Performance Risk System.

   To be compliant with DFARS 252.204-7020 on the CCRA, the following conditions must be met:

   - Questions 3 and 3.a must be Yes
   - Question 3.b must have a valid SPRS assessment date that is less than 3 years old.
   - Question 3.c must have the appropriate confidence level (Basic, Medium, High Onsite, High Virtual) for the SPRS submission.

   See the linked Quick reference guide for instructions on how to submit your DoD Assessment score to SPRS.

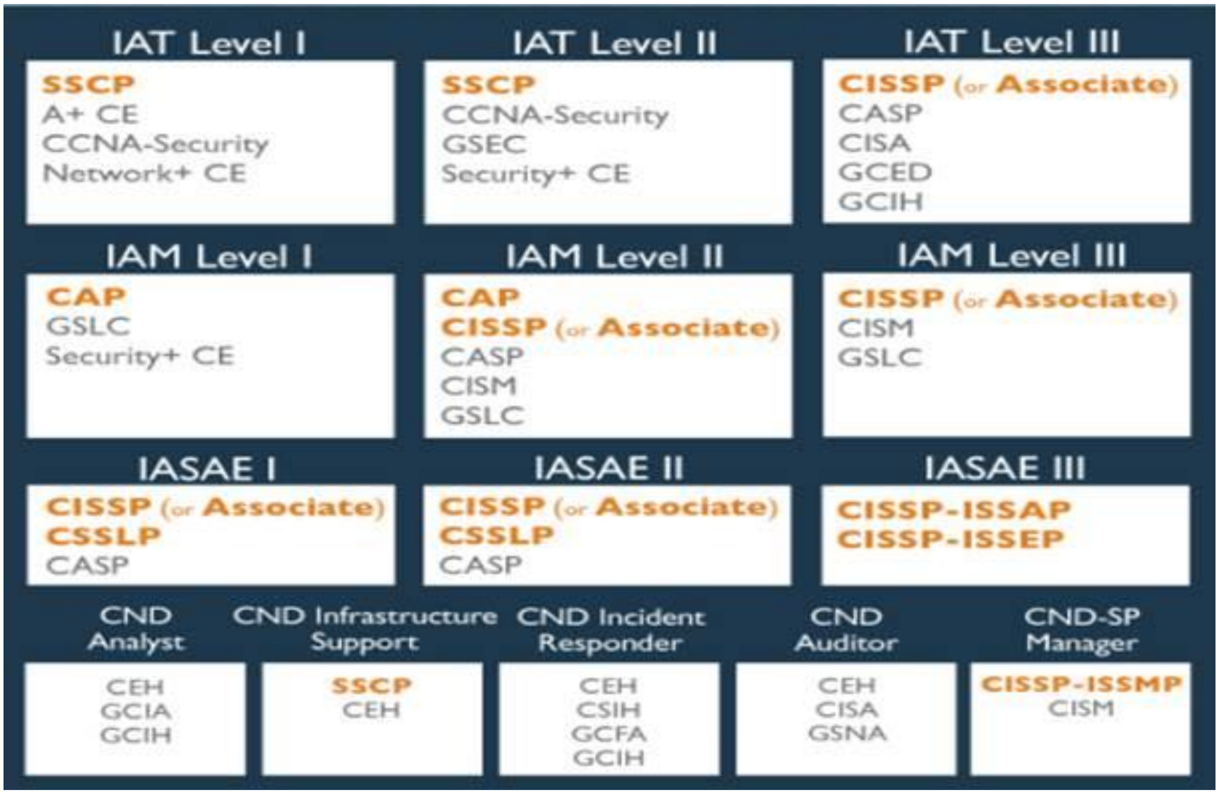
10. **Can we get an electronic (excel) version of the CCRA?**
    The latest version of the CCRA can be found on ND-ISAC CyberAssist Website located here.

Cybersecurity – Supplier’s Frequently Asked Questions

General Questions:

11. **What expertise is needed to understand how to improve my company’s cybersecurity posture.**
    Understanding and improving cyber capability levels require knowledgeable IT and Cyber talent. If the supplier does not have such skills, engaging local IT support companies or outsourcing the IT and Cyber functions should be considered to improve a company’s capability level. Potential criteria for selecting an appropriately qualified support company may include, but not be limited to, ensuring the company’s cyber talent has generally accepted industry certifications. Guidance on the appropriate level of cybersecurity credentials can be found throughout many sources. Two sources are provided for ease of reference. The supplier is encouraged to investigate the full range of sources of cybersecurity credentials.
    1. National Initiative for Cybersecurity Careers and Studies (NICCS). This site provides a comparison of the major cybersecurity certifications.
    2. US Department of Defense (DOD) 8570.01-M provides guidance on various baseline cyber certifications. A baseline certification must be obtained by any supplier members supporting the DoD who have privileged system access performing IA functions (i.e., Information Assurance Technical) or who provide design functions such as Information Assurance System Architecture and Engineering (IASAE).
        a. In addition to the IA baseline certification requirement for their level, IATs or IASAEs who also perform IAT functions must successfully pass the appropriate CE training course (for example a Cisco OS or Linux+ OS training course test). The CE certificate must be obtained through industry vendor-provided training. FedVTE training and other commercial training courses are excellent training venues, but they do not satisfy the requirement for the vendor OS CE baseline certificates.

Cybersecurity – Supplier’s Frequently Asked Questions



IAT Level I	IAT Level II	IAT Level III
SSCP A+ CE CCNA-Security Network+ CE	SSCP CCNA-Security GSEC Security+ CE	CISSP (or Associate) CASP CISA GCED GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
CAP GSLC Security+ CE	CAP CISSP (or Associate) CASP CISM GSLC	CISSP (or Associate) CISM GSLC
IASAE I	**IASAE II**	**IASAE III**
CISSP (or Associate) CSSLP CASP	CISSP (or Associate) CSSLP CASP	CISSP-ISSAP CISSP-ISSEP

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND-SP Manager
CEH GCIA GCIH	SSCP CEH	CEH CSIH GCFA GCIH	CEH CISA GSNA	CISSP-ISSMP CISM

Figure Q2 DoD Directive 8570.1 Cyber Certifications Guidance

With any decision to engage an external company, the supplier should evaluate the company’s reputation, work product, and performance among other business requirements.

For information about why Lockheed Martin is requiring completion of the cyber questionnaires or information on Lockheed Martin’s general supply chain cybersecurity strategy, refer to the Lockheed Martin corporate website and the suppliers link at the top right www.lockheedmartin.com/us/suppliers/cyber-security.html.

12. What resources are available to help a supplier with implementing the NIST controls?

NIST 800-171 Control Guidance

- NIST Special Publication **800-171** Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST Special Publication **800-171A** Assessing Security Requirements for Controlled Unclassified Information
- NIST Special Publication **HB 162** NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements
- NIST SP 800-171 DoD Assessment Methodology
- Cybersecurity Maturity Model Certification (CMMC) Assessment Guides

Documentation Templates

- Example of an *SSP* (**System Security Plan template**) (.docx)
- Example of a basic *POA&M* (**Plan-of-Action-and Milestones template**) (.docx)

Cybersecurity – Supplier's Frequently Asked Questions

Links for *CUI* (Controlled Unclassified Information)

- **CUI Registry**
- An enumerated list of **CUI categories**
- **CUI marking handbook** (.pdf)
- **CFR Title 32 Vol 6 Sec 2002-20** (.pdf)

DoD Cyber **Incident Reporting** for contractors and subcontractors

DIBSCC CyberAssist Webpage – is a repository of publicly available resources to help implement and assess cybersecurity controls.

13. **I am a provider of consulting services and/or labor resources. Am I required to complete the CCRA?**
    Within services contracts, such as consulting services or experienced non-Lockheed Martin labor resources, it is generally assumed that Lockheed Martin Sensitive Information is shared. It can be further assumed that if there is an executed Non-Disclosure Agreement (NDA) or similar legal construct then Sensitive Information is shared. If the supplier's employees process, store, and or transmit such sensitive information exclusively using Lockheed Martin's IT assets then the cybersecurity assessment is not required. If the supplier's employees process, store and or transmit such sensitive information using *any of* the supplier's IT assets then the cybersecurity self-assessment *must be completed.*

    Questions as to specifics about the information shared by Lockheed Martin and your company should be addressed directly with your Lockheed Martin primary engagement interface.

14. **We currently do not hold any contracts with LM, do we still have to complete this requirement?**
    If you have in the past, currently, or will in the future; store, process, or transmit Lockheed Martin Sensitive Information to include DoD Controlled Unclassified Information (CUI) you are required to complete the CCRA regardless of holding contracts with Lockheed.

    Lockheed Martin will use the response to these surveys as a basis of evaluation for future supplier selections and contract commitments.

Reminder notices from Exostar and Lockheed Martin

15. **Why do I keep receiving follow up/reminder emails from Lockheed Martin and Exostar?**
    If you are receiving follow-up emails after completing the questionnaire, then a review of our records indicated that you have not satisfied all the cybersecurity requirements. Please review your Trading Partner Manager (TPM) vendor profile and Onboarding Module (OBM) accounts to ensure that all questions have been properly updated, saved, and submitted.

    Please use the ***OBM Guidance for TPM Users*** guide on the following Exostar Resource webpage: https://www.myexostar.com/?ht_kb=tpm-training-resources (User Guide) with the following review steps:

Trading Partner Manager Review:

1. Log into TPM and navigate to the Self-Certification section (User Guide Step 1 -2)
2. Review and update "Cyber Security" information. (User Guide Step 3)
3. **Ensure that the *Applicability of Cyber DFARS and NIST SP 800-171* and *Handling Sensitive Information* sections are not blank or null.** (User Guide Step 3)
4. Save and update your response.

Onboarding Module Review:

1. Complete Steps 1 through Step 4 from above.
2. Click on either ***Click here to view or update the Cybersecurity Compliance and Risk Assessment (CCRA) questionnaire*** to be linked to the OBM Dashboard. (see ***Supplier Organization User Guide*** on the following Exostar Resource webpage: https://www.myexostar.com/?ht_kb=onboarding-module-training-resources)
3. Accept **Export Control Acknowledgement**.
4. Click on the **Pending Forms** widget and select the ***CCRA FORM***
   a. **IMPORTANT NOTE:** If the Form Request status is stuck at 20%, you can select the options menu **[three dots]** and ***reassign*** it to the user. This will increase the request status to 40% and enable form editing.
5. Ensure that you go to the end of each questionnaire and click on the ***Save*** and then ***Submit*** button to save and submit the questionnaire for scoring.
6. Instructions on how to complete the questionnaire can be found in the ***Supplier Organization User Guide*** on the following Exostar Resource webpage: https://www.myexostar.com/?ht_kb=onboarding-module-training-resources

16. I've already completed the questionnaires, but I am still receiving reminder notices.

In addition to completing the questionnaires, suppliers are required to keep questionnaires current (updated within the last 12 months). Upon receipt of reminder notices the supplier must log back into Exostar, make updates to their questionnaire, and re-submit the questionnaire to complete this requirement.

For instructions on how to update/complete the questionnaire, please use the ***Supplier Organization User Guide*** on the following Exostar Resource webpage: https://www.myexostar.com/?ht_kb=onboarding-module-training-resources.

Replication: Form Groups

17. We have more than one business unit that are suppliers to Lockheed Martin with accounts in Exostar, do we have to manually complete the questionnaires for each account?

No, Exostar's Form Group function has been developed to allow organizations to share the completed CCRA across multiple business units. Lockheed Martin requires that companies with multiple entities must manage IT and cybersecurity centrally across all eligible entities. Furthermore, all eligible related entities must be governed by the same centralized IT and cybersecurity policies. If your company meets those eligibility requirements, then your company can be configured for From Grouping.

The process for requesting Form Group is provided here: https://myexostar.com/?ht_kb=pim-supplier-information#form-grouping

The completed spreadsheet should be submitted to Exostar Online Support.

18. **I've already completed the Form Group request for my organization's account but need to add or remove accounts from this form group because they are no longer part of our organization.**
    To add accounts to an existing form group, you must complete the form group request using the same master account previously used and add the additional accounts you need to the destination account fields. Once completed, submit the new request to Exostar Online Support.

    To remove the account(s) from an existing form group, please contact Exostar Online Support

TPM related questions:

19. **How do I get to the TPM portal?**
    Please use the ***OBM Guidance for TPM Users*** guide on the following Exostar Resource webpage: https://www.myexostar.com/?ht_kb=tpm-training-resources (User Guide)

20. **I've answered "Yes" to both the *Applicability of Cyber DFARS and NIST SP 800-171* and *Handling Sensitive Information* sections, but I am still unable to access PIM to complete the questionnaires.**
    Please contact Exostar Online Support

OBM Related Questions:

21. **How can I access and complete the CCRA on OBM?**
    Suppliers can gain access to the questionnaires by following the instructions below:

    1. Log in to the TPM portal and update your Cybersecurity profile. (Steps 1 through 2: ***OBM Guidance for TPM Users Guide*** on the following Exostar Resource webpage: https://www.myexostar.com/?ht_kb=tpm-training-resources (User Guide))
    2. Navigate to the ***Self-Certification*** section of your TPM vendor profile.
    3. Answer the question in the *Applicability of Cyber DFARS and NIST SP 800-171* section. If you are required to be compliant with DFARS 252.204-7012, then the answer to this question will be "(1)." If not, select one of the applicable "(2)" options provided.
        a. If you've answered "(1)" you will be provided with a hyperlink, ***Click here to view or update the Cybersecurity Compliance and Risk Assessment (CCRA) questionnaire***.
        b. If you've answered "(2) *x*" no further action for the CCRA questionnaire is required.
    4. Answer the question in the *Handling Sensitive Information* section. If you are handing Sensitive Information from LM, then select Yes.

   a. Use ***Click here to view or update the Cybersecurity Compliance and Risk Assessment (CCRA) questionnaire*** to access and complete the questionnaire.
   b. If you've answered "No," no further action for the CCRA is required.
5. Once you've logged into the OBM portal, please use the ***Supplier Organization User Guide*** from the Onboarding Module Training Resources page for detailed instructions on how to complete/update the questionnaires.
6. Should the Org Admin want to delegate the completion of the questionnaire to another member of your organization, they can do so by following the directions on Page 50 of the *MAG User Guide* provided here: https://www.myexostar.com/?ht_kb=mag-training-resources

22. I can see the Questionnaire(s) on the OBM dashboard, but how can I start responding?

To complete the questionnaire, you must **assign** the questionnaire to the appropriate personnel responsible for completing it. If the CCRA form is showing as 20% provisioned, use the 3-dot option menu to select ***Reassign*** it to the appropriate user. This should change the provision status to 40% and make the form accessible.

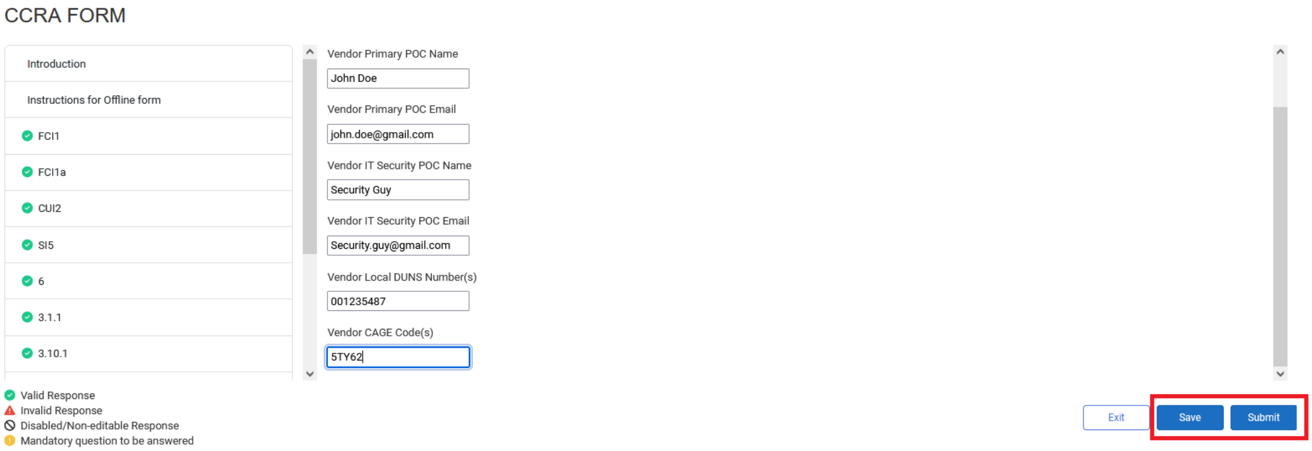
Please use the *Supplier Organization User Guide* from the Onboarding Module Training Resources page for detailed instructions on how to assign the CCRA.

23. I've completed the questionnaires but my LM Buyer/Subcontract Administrator says that it is not completed on their systems.

Ensure that the supplier has clicked on the ***Save*** and then the ***Submit*** button at the end of the questionnaire. This will submit the questionnaire for scoring and push updates to integrated systems.

Instructions on how to complete the questionnaire can be found in the ***OBM Guidance for TPM Users*** guide on the following Exostar Resource webpage: https://www.myexostar.com/?ht_kb=tpm-training-resources

Screenshot of the ***Save*** and ***Submit*** button located only at the end of each questionnaire:



CCRA FORM

Vendor Primary POC Name: John Doe

Vendor Primary POC Email: john.doe@gmail.com

Vendor IT Security POC Name: Security Guy

Vendor IT Security POC Email: Security.guy@gmail.com

Vendor Local DUNS Number(s): 001235487

Vendor CAGE Code(s): 5TY62

✓ Valid Response
⚠ Invalid Response
⦸ Disabled/Non-editable Response
● Mandatory question to be answered
Exit
Save
Submit